# Release Notes

/ ForgeRock Access Management 6.5

Latest update: 6.5.5

ForgeRock AS.
201 Mission St., Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

## Abstract

Notes covering new features, fixes and known issues in ForgeRock® Access Management. ForgeRock Access Management provides authentication, authorization, entitlement, and federation software.

# Table of Contents

# Preface

Read these release notes before you install ForgeRock Access Management or update your existing installation.

The information contained in these release notes cover prerequisites for installation, known issues and improvements to the software, changes and deprecated functionality, and other important information.

## About ForgeRock Identity Platform™ Software

ForgeRock Identity Platform™ serves as the basis for our simple and comprehensive Identity and Access Management solution. We help our customers deepen their relationships with their customers, and improve the productivity and connectivity of their employees and partners. For more information about ForgeRock and about the platform, see https://www.forgerock.com.

Chapter 1

# What's New

This chapter covers new features and improvements in ForgeRock Access Management 6.5.

## Maintenance Releases

ForgeRock maintenance releases contain a collection of fixes and minor RFEs that have been grouped together and released as part of our commitment to support our customers. For general information on ForgeRock's maintenance and patch releases, see Maintenance and Patch Availability Policy.

AM 6.5.5 is the latest release targeted for AM 6.5 deployments, and can be downloaded from the ForgeRock Backstage website. To view the list of fixes in this release, see Key Fixes in AM 6.5.5.

The release can be deployed as an initial deployment or updated from an existing 6.5.x deployment; see "Supported Upgrade Paths".

## New Features

### *New Features in AM 6.5.5*

- `org.forgerock.openam.encryption.padshortinputs` system property for AES Key Wrap encryption

  A new Java system property (`org.forgerock.openam.encryption.padshortinputs`) pads short inputs to help ensure future compatibility with Java 17 when upgrading.

  For details, see "Preparing AES Key Wrap Encryption" in the *Installation Guide*.

- New JWKs URI for remote consent agents

  To make it easier to publish keys used for remote consent, AM 6.5.5 provides a new JWKs URI, specifically for remote consent agents. This URI indicates where a remote consent service can obtain the keys that AM uses to sign and encrypt the consent request. These keys include:

  - The public signing key, used to sign the consent request that is sent to the remote consent server, so that it can be validated on the remote consent server.
  - The public encryption key for the consent response, so that the response can be encrypted (if encryption is enabled).

The default JWKs URI for remote consent clients is `/oauth2/consent_agents/jwk_uri`.

For example, `https://openam.example.com:8443/openam/oauth2/realms/root/realms/alpha/consent_agents/jwk_uri`.

### *New Features in AM 6.5.4*

- New Properties Available to Claims and Access Token Scripts

  AM 6.5.4 adds new properties to the *OpenID Connect Claims* and *OAuth 2.0 Access Token Modification* script types, for accessing the properties of the relevant client, and the incoming request.

  For more details, see "Scripting OpenID Connect 1.0 Claims" in the *OpenID Connect 1.0 Guide* and "Modifying the Content of Access Tokens" in the *OAuth 2.0 Guide*.

- New versions of SSOAdminTools and SSOConfiguratorTools

  SSOAdminTools 5.1.2.19 and SSOConfiguratorTools 5.1.2.19 are now compatible with AM 6.5.4. For download and installation instructions, see "Obtaining Software" in the *Installation Guide*.

- New Use Force Authentication setting

  The Advanced OpenID Connect options for an OAuth 2.0 Provider now includes the setting Use Force Authentication for `prompt=login`. The setting applies only to module and chain implementations where `prompt=login` is specified. For details, see "Advanced OpenID Connect" in the *OpenID Connect 1.0 Guide*.

- `org.forgerock.openam.authentication.forceAuth.enabled` advanced server property for authentication chains

  A new advanced server property (`org.forgerock.openam.authentication.forceAuth.enabled`) controls the `ForceAuth` authentication property for chains.

  For details, see `org.forgerock.openam.authentication.forceAuth.enabled` in the *Reference*.

### *New Features in AM 6.5.3*

- Added Local Storage Support for SAML v2.0 Single Sign-on

  AM 6.5.3 stores SAML v2.0 single sign-on progress state as client-side data when using web browsers that support local storage, removing the need to use sticky load balancing.

  As part of this change, AM's web application now includes a new URL servlet pattern definition (`/saml2/continue/*`) and a new `.jsp` file (`idpReadFromStorage.jsp`) to support the local storage functionality.

  Ensure that your firewalls and reverse proxies are configured to allow access to these locations.

  For more information, see "Session State Considerations" in the *SAML v2.0 Guide*.

- New Agents Notifications

  AM 6.5.3 now lets agents receive notifications for OAuth2 access token revocations. Two new revocation notifications are introduced:

  - `/oauth/revoke/grant`. Occurs when grant is being revoked.
  - `/oauth/revoke/token`. Occurs when the access token is being revoked.

  The notifications include either the `authGrantId` for grant notifications or the `auditTrackingId` for access token notifications, for example:

  ```
  { "authGrantId": "ofEsx2EJBYPdRWxNK0xr0EsLd-0" }
  ```

  ```
  { "auditTrackingId": "2453cd20-c9f5-45ea-b307-7345002e1f55-36063" }
  ```

  The `/oauth2/tokeninfo` endpoint response now includes the `authGrantId` to let clients, like IG, that might be caching access tokens to track when a grant has been revoked.

- Extended Scripted Node for Auditing

  AM 6.5.3 introduces a Scripted Node extension to include a custom message in the audit logs that describes the node and its outcome.

  The Scripted Node now has a `auditEntryDetail` variable where you can set as a String or Map value. The Scripted Node uses the value when it writes to the audit logs.

- Let `wreply` Parameter Use URLs Added to a Valid wreply List

  AM 6.5.3 now lets the `wreply` parameter in the call use URLs added to a Valid `wreply` List.

  For more information, see OPENAM-15548: WS-Fed - allow wreply to use Valide wreply List

- Added Endpoint to Get Session Information and Also Reset Idle Timeout

  AM 6.5.3 includes a new `getSessionInfoAndResetIdleTime` endpoint that resets the idle timeout when obtaining information about a session. The existing `getSessionInfo` endpoint does not reset the idle timeout.

  For more information, see "Obtaining Information About Sessions" in the *Authentication and Single Sign-On Guide*.

- Ability to Configure a Failure URL in Server-Side Authentication Scripts

  Server-side scripts can now redirect users to a specific URL after authentication failure. For more information, see "Redirecting the User After Authentication Failure" in the *Authentication and Single Sign-On Guide*.

- New Account Active Check Authentication Module

AM 6.5.3 includes a new Account Active Check authentication module, which lets you determine whether an account is marked as active, or locked, without having to run through the remainder of the authentication chain.

For more details, see "Account Active Check Module" in the *Authentication and Single Sign-On Guide*.

- Forgotten Password REST API Endpoint Requires Code

  The User Self-Service Forgotten Password REST endpoint now requires a `code` value when specifying a new password.

  For more details, see "Resetting Forgotten Passwords" in the *User Self-Service Guide*.

### *What's New in AM 6.5.2.3*

- There are no new features in this release, only bug fixes.

### *What's New in AM 6.5.2.2*

- There are no new features in this release, only bug fixes.

### *What's New in AM 6.5.2.1*

- There are no new features in this release, only bug fixes.

### *What's New in AM 6.5.2*

- Added Support for the JWT Profile for OAuth 2.0 Authorization Grant

  AM 6.5.2 adds support for the JWT profile for OAuth 2.0 Authorization Grant, defined in the *RFC 7523* specification.

  As part of this feature, AM includes a new agent of the type Trusted JWT Issuer.

  For more information, see "JWT Profile for OAuth 2.0 Authorization Grant" in the *OAuth 2.0 Guide*.

- Added OAuth 2.0 Access Token Modification Scripts

  AM 6.5.2 adds support for scripting the modification of issued OAuth 2.0 access tokens. You can add properties to the access token, for example, values taken from the resource owner's profile, such as telephone number or email address.

  For more information, see "Modifying the Content of Access Tokens" in the *OAuth 2.0 Guide*.

- Added OpenID Connect Client Initiated Backchannel Authentication (CIBA) Support

AM 6.5.2 introduces support for OpenID Connect Client Initiated Backchannel Authentication (CIBA) that allows a client application, known as the *consumption device*, to obtain authentication and consent from a user without requiring the user to interact with it directly. The user authenticates and consents to the operation using a separate "decoupled" device, known as the *authentication device*, such as an authenticator application or a mobile banking application on their mobile phone.

For more information, see "Backchannel Request Grant" in the *OpenID Connect 1.0 Guide*

- Added Support for the `id_token_hint` Parameter on the OAuth 2.0/OpenID Connect Authorization Endpoint

  AM 6.5.2 adds support for client relying parties to use the `id_token_hint` parameter in their request to the authorization endpoint as a hint about the end user's session. AM uses the ID token to verify whether the end user specified on it has a valid session in AM.

  As part of this change, the authorization endpoint supports the new `none` response type.

  For more information, see "/oauth2/authorize" in the *OAuth 2.0 Guide* and "Retrieving Session State without the Check Session Endpoint" in the *OpenID Connect 1.0 Guide*.

### *What's New in AM 6.5.1*

- OAuth 2.0 Mutual TLS (mTLS) Support

  AM 6.5.1 adds support for draft 12 of the OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens specification, a key component of ForgeRock's Open Banking and Revised Payment Services Directive (PSD2) support.

  For information about authenticating an OAuth 2.0 client using mTLS certificates, see "Authenticating Clients Using Mutual TLS" in the *OAuth 2.0 Guide*.

  For information about issuing certificate-constrained OAuth 2.0 access tokens, see "Certificate-Bound Proof-of-Possession" in the *OAuth 2.0 Guide*.

- New Extension Point to Customize Public Key ID (`kid`)

  By default, AM generates a key ID (`kid`) for each public key exposed in the `jwk_uri` URI when AM is configured as an OAuth 2.0 authorization server.

  AM 6.5.1 introduces a new extension point, `KeyStoreKeyIdProvider`, to customize the key ID values associated with public keys stored in keystore secret stores.

  For more information, see "Customizing Public Key IDs" in the *OpenID Connect 1.0 Guide*.

- OAuth 2.0 Dynamic Client Registration Management Protocol (RFC7592) Fully Supported

  AM 6.5.1 adds support for OAuth 2.0/OpenID Connect clients to edit and delete their client profile data as per RFC7592.

Earlier versions of AM offered support for read operations only.

For more information, see "Dynamic Client Registration Management" in the *OAuth 2.0 Guide*.

- Updated Versions of the Admin Tools and Configurator Tools Utilities

  AM 6.5.1 also includes an updated version of the Admin Tools (`AM-SSOAdminTools-5.1.2.3.zip`) and the Configurator Tools (`AM-SSOConfiguratorTools-5.1.2.3.zip`) utilities. These upgraded versions of the tools fixes an issue that could cause the **ssoadm** to malfunction while using JDK 11 or JDK 1.8.0_192+ (see Known Issues in AM 6.5). You can download these versions from the *ForgeRock Backstage* website.

### *What's New in AM 6.5*

ForgeRock Access Management 6.5 is a major release that introduces new features, functional enhancements, and fixes.

- Secret Stores

  AM introduces secret stores, which are repositories for cryptographic keys, key pairs, and credentials, such as passwords. The OAuth2 providers and the Persistent Cookie Module are now using secret stores.

  AM 6.5 adds support for the following secret store types:

  - Keystore

    AM supports a number of different keystore formats, including JCEKS, JKS, PKCS11, and PKCS12. AM allows key rotation within keystore secret stores.

  - File System Secret Volumes

    AM supports secrets that are stored as files in defined folders. For example, in a cloud deployment you could mount a secret volume that AM can access.

  - Hardware Security Modules (HSM)

    AM supports retrieval of secrets from hardware security modules, either locally or over the network.

  AM also supports secrets stored as environment or system properties.

  After an upgrade to AM 6.5, the following secret stores are deployed and configured for you:

  - `default-keystore`
  - `default-password-store`

If you had Persistent Cookie authentication modules or OAuth 2.0 Providers configured, AM will perform extra tasks to ensure that the upgrade configures your secret stores correctly.

For more information, see "*Configuring Secrets, Certificates, and Keys*" in the *Setup and Maintenance Guide*.

- Added Support for Web Authentication (WebAuthn)

  AM 6.5 adds support for Web Authentication, which allows users to authenticate by using an authenticator device as a second factor, for example the fingerprint scanner on their laptop or phone.

  For more information about Web Authentication, see "About Web Authentication (WebAuthn)" in the *Authentication and Single Sign-On Guide*.

  For information about the parts of the Web Authentication specification that are not currently supported, see Web Authentication (WebAuthn) Limitations.

- Added Support for External Policy and Applications Configuration Store

  AM 6.5 adds support for using external DS directory servers instead of the embedded instance for storing the following data:

  - Policy data. Policy-related data, such as policies, policy sets, and resource types.
  - Application data. Application-related data, such as web and Java agent configuration, federation entities and configuration, and OAuth 2.0 client definitions.

  For more information, see "Preparing Policy and Application Stores" in the *Installation Guide*.

- Added Support for the Directory Services Entry Expiration and Deletion Feature to Manage CTS Tokens

  AM 6.5 adds support to configure the DS entry expiration and deletion feature to manage CTS tokens. This configuration frees AM resources in the AM servers that can then be used for policy or authorization requests.

  Two possible configurations are supported:

  - DS manages the time to live for all tokens in the CTS and the AM CTS reaper is disabled.

    Disabling the AM CTS reaper completely impacts session-related functionality, such as sending notifications about session expiration or session timeout to agents.

  - The AM CTS reaper manages a subset of the tokens in the CTS, usually the `SESSION` tokens, while DS manages the non-session tokens.

    This configuration ensures your environment can still make use of all session functionality, while benefiting from DS's capabilities as well.

For more information, see "Configuring the CTS Reaper" in the *Installation Guide*.

- Improved CTS Storage Scheme for OAuth 2.0 tokens

  AM 6.5 introduces a new scheme for storing OAuth 2.0 tokens in the CTS store, called the *grant-set* scheme.

  The `grant-set` scheme groups multiple authorizations for a given OAuth 2.0 client and resource owner pair and stores them in a single CTS `OAUTH2_GRANT_SET` entry. This implementation reduces the size and quantity of entries stored, as well as the number of calls required to perform OAuth 2.0 operations.

  The `one-to-one` scheme, which stores the state of multiple authorizations for a given OAuth 2.0 client and resource owner pair across multiple entries, will be removed in a future release. You should upgrade to the `grant-set` scheme once all the servers on your environment have been upgraded to AM 6.5 or later.

  The `grant-set` scheme is backwards-compatible with existing entries stored in the CTS store. Therefore, any access or refresh token issued before configuring the `grant-set` scheme is still valid. Existing tokens will be retained in their original form until the refresh token expires or it is actively revoked.

  **Note**

  AM 6.5 also introduces a new `"cts"` claim for OAuth 2.0 access tokens. This claim allows AM to identify the storage schema for the presented token.

  If the claim is not present, for example, when tokens are issued before the `grant-set` feature was introduced in this release, then the previous storage scheme will be selected. If the claim is present, the AM will select the correct storage scheme for that particular token. This claim was added to ensure that the AM is backwards-compatible with the previous access tokens.

  Users will not notice any change in the tokens they receive, and there is no change to the OAuth 2.0 endpoints.

  To enable the `grant-set` scheme, navigate to Configure > Global Services > OAuth2 Provider > Global Attributes and set the CTS Storage Scheme drop-down to Grant-Set Storage Scheme. Then, save your changes.

  New OAuth 2.0 tokens stored in the CTS after the change will use the new scheme automatically.

- Added Support for Customizing User-Facing OAuth 2.0 Pages

  AM 6.5 now supports the `logo_uri`, `client_uri`, and `policy_uri` parameters for OAuth 2.0 clients as defined in RFC 7591.

  Use these parameters to customize the OAuth 2.0 user-facing pages. For more information, see "Advanced" in the *OAuth 2.0 Guide*.

- New OAuth 2.0 Provider Properties Added

  AM 6.5 adds a number of new OAuth 2.0 Provider properties, as follows:

  - Properties for controlling the supported signing and encryption algorithms and methods.
  - A property for controlling the supported signing algorithms for the `private_key_jwt` JWT-based authentication method.
  - A property for controlling the supported grant types.

  For more information about the properties available in OAuth 2.0 providers, see "OAuth2 Provider" in the *OAuth 2.0 Guide*.

- New Authentication Nodes Added

  AM 6.5 introduces the following authentication nodes, in addition to the nodes added for Web Authentication (WebAuthn) and for displaying device recovery codes:

  - Agent Data Store Decision Node
  - Cookie Presence Decision Node
  - Message Node

- Added Support for Audit Logging to a PostgreSQL Database

  AM 6.5 adds support for recording audit events to a PostgreSQL database. An SQL script is provided to help in setting up the required tables.

  For information, see "Implementing JDBC Audit Event Handlers" in the *Setup and Maintenance Guide*.

# Major Improvements

### *Improvements in AM 6.5.5*

- Improved locale assessment for message nodes

  The "Message Node" in the *Authentication and Single Sign-On Guide* now has better assessment of the locale to use when displaying messages to the user.

- Additional Improvements in AM 6.5.5

  - OPENAM-17600: XForwardedHeadersBaseURLProvider fallback on scheme and port
  - OPENAM-16732: Choice Collector Node is not part of the am-external repo

- OPENAM-15997: Enhance CookieHelper to perform better cookie detection

### *Improvements in AM 6.5.4*

- The JWK URI Endpoint Can Now Return Duplicate Key IDs

  Earlier versions of AM removed the `alg` parameter from the keys returned by the `jwk_uri` endpoint.

  Removing the `alg` parameter ensures that each key ID (`kid`) exposed by the endpoint matches a unique key, as recommended by the RFC7517 specification.

  AM 6.5.4 includes a toggle, Include all kty and alg combinations in jwk_uri, that lets the endpoint display duplicate key IDs with their corresponding `alg` and `kty` parameters.

  The toggle property is disabled by default.

  For more information, see "Displaying Every Algorithm and Key Type Associated to a Key ID" in the *OpenID Connect 1.0 Guide*.

- Improved Client Connection Handling

  AM 6.5.4 improves the way its ClientHandler code handles connection pools and timeouts. This affects client connections that AM opens against third parties, such as social identity providers.

  As part of this change, AM includes the following new advanced server properties:

  - `org.forgerock.openam.httpclienthandler.system.clients.connection.timeout`
  - `org.forgerock.openam.httpclienthandler.system.clients.max.connections`
  - `org.forgerock.openam.httpclienthandler.system.clients.pool.ttl`
  - `org.forgerock.openam.httpclienthandler.system.clients.response.timeout`
  - `org.forgerock.openam.httpclienthandler.system.clients.retry.failed.requests.enabled`
  - `org.forgerock.openam.httpclienthandler.system.clients.reuse.connections.enabled`

  For more information, see "Advanced Properties" in the *Reference*.

- Improvements to the OTP Email Sender Node

  On earlier versions of AM, the amount of time that the "OTP Email Sender Node" in the *Authentication and Single Sign-On Guide* waited to declare that an outbound SMTP connection was unavailable depended on the operating system where AM ran.

  AM 6.5.4 includes the following advanced server properties to configure the timeout:

  - `org.forgerock.openam.smtp.system.connect.timeout`

- `org.forgerock.openam.smtp.system.socket.read.timeout`
- `org.forgerock.openam.smtp.system.socket.write.timeout`

For more information, see Advanced Properties in the *Reference*.

- Changes to the Retry Limit Decision Node

  The "Retry Limit Decision Node" in the *Authentication and Single Sign-On Guide* can now persist the number of failed login attempts in the identity store between successful authentications.

  To support this change, the following LDIF schema files have been updated:

  - `ad_user_schema.ldif`
  - `adam_user_schema.ldif`
  - `odsee_user_schema.ldif`
  - `opendj_remove_user_schema.ldif`
  - `opendj_user_schema.ldif`
  - `tivoli_user_schema.ldif`

  Moreover, a new file, `opendj_retry_limit_node_count.ldif`, has been added to the AM deliverables, and the DS identity setup profile has been updated.

  The new functionality is not enabled by default because it requires schema changes to the identity store. But, ForgeRock recommends that you enable it to harden the security around this node.

  To enable the Save Retry Limit to User feature, first apply the schema changes in the `opendj_retry_limit_node_count.ldif`file to the identity store. Then reconfigure the "Retry Limit Decision Node" in the *Authentication and Single Sign-On Guide*.

  For more information, see "*Upgrading AM Instances*" in the *Upgrade Guide*.

- Additional Improvements in AM 6.5.4
  - OPENAM-11160: Allow Amster to work on non-https fqdn when secure cookie is set.
  - OPENAM-11687: Allow delegated admin to query authorized apps of a user
  - OPENAM-12242: Correctly Error RP Initiated Logout
  - OPENAM-12886: Allow configurable audience for clients authenticating using JWT
  - OPENAM-14220: Improve reporting of upgrade failures of Base64-encoded values
  - OPENAM-14903: Storing additional information in OAuth2.0 Client

- OPENAM-14915: Ability to access more OAuth2 configuration or parameters in OIDC/OAuth2 scripts
- OPENAM-15704: Suppress redundant log messages introduced via fix for OPENAM-14050.
- OPENAM-16961: OIDC Claims Script - /userinfo to access clientProperties
- OPENAM-17096: HTTP GET at the JWK URI to get the public signing key - response does not have "alg" attribute
- OPENAM-17151: Extend the IDPAuthnContextMapper interface to access the http request object
- OPENAM-17235: Debug logging with trace level should show some perf stats
- OPENAM-17430: Prevent FederationPlugin doing unnecessary schema change
- OPENAM-17547: Prevent duplicate reads identified in StatelessTokenStore
- OPENAM-17721: OAuth2 Device grant - scope is missing from token response
- OPENAM-17813: Allow /userinfo endpoint to include 'aud' claim in response
- OPENAM-17898: Additional diagniostic logging for UMA policy subject comparison

### *Improvements in AM 6.5.3*

- OPENAM-476: Allow AssertionConsumerURL with dynamic elements
- OPENAM-12149: Allow for SAML IdP entities to have same name in different realms
- OPENAM-12184: Extend the DJ/DS SDK affinity LB feature to the userstore connection
- OPENAM-13317: Enable Authentication trees to display custom error messages
- OPENAM-13378: Authentication Tree does not retrieve User Attributes & Session Properties From Session via REST API.
- OPENAM-14317: Request to enhance how registered resource types are referenced from applications
- OPENAM-14803: Support UI-defined WebAuthn integration
- OPENAM-14939: Enable "org.apache.xml.security.ignoreLineBreaks=true" by default
- OPENAM-15021: Fallback to non-proxied Authz update when Proxied authorization update fails
- OPENAM-15379: Clear the messages pop-up upon successful authentication.
- OPENAM-15388: Session upgrade from AuthN tree to include "Anonymous User Mapping"

- OPENAM-15433: Make the endSession endpoint continue flow when presented with valid id_token but expired session
- OPENAM-15640: Provide session idle refresh option when requesting session info
- OPENAM-15695: Include authGrantId in response when calling /introspect endpoint with an access token
- OPENAM-15732: Create a new setting to store the default SAML key transport algorithm
- OPENAM-15899: Have an option to add <ds:X509Certificate> tag in the signed SLO request
- OPENAM-15962: WebAuthn Nodes: Make Origin Domains configuration optional.
- OPENAM-15996: CTS - External Token Store does not support StartTLS
- OPENAM-16018: Scripted Decision Node API must support to HTTP URL Request Parameters
- OPENAM-16051: OAuth2Client config - _queryFilter accepts only 'true'
- OPENAM-16062: Update Apache XML Security For Java to v2.1.5
- OPENAM-16098: Have FR OATH OTP use removed padded Base32 format for the otpauth
- OPENAM-16146: Auditing details of user/group updates impacts performance - add option to turn it on
- OPENAM-16183: Document How to have AM Java SDK return a Affinity connection pool
- OPENAM-16349: Include support for new "am-introspect-all-tokens-any-realm" scope in IG Agent configuration

### *Improvements in AM 6.5.2.3*

- OPENAM-15444: Prepare for Chrome's move to SameSite=lax by default
- OPENAM-15841: DisableSameSiteCookiesFilter broken on WebLogic

  These fixes add a new filter that sets the `SameSite=None` attribute for all secure AM cookies on compatible browsers. For more information on the SameSite cookie support, see the *ForgeRock Knowledge Base* website.

### *Improvements in AM 6.5.2.2*

- There are no major improvements to existing functionality other than bug fixes.

### *Improvements in AM 6.5.2.1*

- There are no major improvements to existing functionality other than bug fixes.

### *Improvements in AM 6.5.2*

- See What's New in AM 6.5.2 for a list of important changes to existing functionality.

### *Improvements in AM 6.5.1*

- Transactional Authorization Can Return HTTP 401 Messages on Authentication Failure

  In earlier versions of AM, a transactional authorization advice that failed due to invalid credentials always returned an HTTP 200 message.

  Then, the user would be redirected to the protected resource, where policy evaluation would fail.

  AM 6.5.1 introduces a new advanced server property to control whether transactional authorization should return an HTTP 200 or an HTTP 401 message depending on the needs of your environment.

  In both cases, users cannot access the protected resources when they fail to complete the required actions during transactional authorization.

  For more information, see the `org.forgerock.openam.auth.transactionalauth.returnErrorOnAuthFailure` advanced server property.

- **New OpenID Connect Authentication Node Added**

  AM introduces an OpenID Connect authentication node for authenticating users from an OpenID Connect-compliant identify provider. For more information, see "OpenID Connect Node" in the *Authentication and Single Sign-On Guide*

- **Option for `isInitiator=false` to WDSSO Configuration**

  AM 6.5.1 now implements the JDK `isInitiator` parameter in the AM WDSSO module, which is used for the JDK Kerberos `LoginModule`. If set to True, it will be in an initiator role. If set to False, it will be in an acceptor role. Default is true.

  For more information, see "Windows Desktop SSO Authentication Module Properties" in the *Authentication and Single Sign-On Guide*

- **Allow `XForwardedHeadersBaseURLProvider` to Fall Back to Host Header**

  When using SSL offloding in the Google Cloud Environment (GCE), the `x-forwarded-for` and `x-forwarded-proto` headers are added, but previously, the `x-forwarded-host` header was not automatically added. This caused origin mismatch failure in web authentication trees.

  AM 6.5.1 now allows the `XForwardedHeadersBaseURLProvider` header to fall back to the host header if `X-Forwarded-Host` is not present.

- **More Data Added to Scripted Node Decision Binding**

  AM 6.5.1's scripted decision node now provides additional access to the following objects:

- `sharedState`
- `transientState`
- `callbacks`
- `requestHeaders`
- `logger`
- `httpClient`
- `realm`
- `existingSession` (if it exists)

- **JWK Key "use" Updated to Include "tls" Type**

  AM 6.5.1 now includes a "tls" type as a supported value for the JSON Web Key (JWK)'s `use` parameter, which specifies the intended use of the public key. Possible values are: `sig`, `enc`, and `tls`.

- **Support for Dynamic Registration PUT**

  AM 6.5.1 supports the a Dynamic Registration PUT to allow a registered OIDC client to update their registration.

- Scripted Authentication Nodes Can Access Additional Functionality

  AM 6.5.1 adds support for the scripted authentication node to use callbacks, and additional features, such as access to `transientState`.

  For more information, see "Scripted Decision Node API Functionality" in the *Authentication and Single Sign-On Guide*.

- **New State Metadata Node Added**

  AM introduces a State Metadata authentication node that returns shared state values as metadata. For more information, see "State Metadata Node" in the *Authentication and Single Sign-On Guide*.

### *Improvements in AM 6.5.0.2*

- There are no major improvements in functionality in this release, other than those listed in Improvements in AM 6.5.0.1 and Improvements in AM 6.5.

### *Improvements in AM 6.5.0.1*

- **OIDC Claims Script Support**

  Additional support has been added to allow `httpClient` within the OIDC Claims script, if desired.

*Improvements in AM 6.5*

- **OAuth 2.0/ OpenID Connect 1.0**
  - **OAuth 2.0 Clients can be Restricted to a Particular OAuth 2.0 Grant Flow**

    In earlier versions of AM, OAuth 2.0 clients could not be restricted to use a particular OAuth 2.0 grant flow and supported any OAuth 2.0 flow without any special configuration.

    OAuth 2.0 clients created in AM 6.5 are assigned the Authorization Code Grant flow by default. You must configure the client if it requires a different flow by navigating to Realms > *Realm Name* > Applications > OAuth 2.0 > *Client Name* > Advanced, and then editing the Grant Types field.

    After an upgrade to AM 6.5, all grant flows are added to existing clients to maintain backwards compatibility.

    For more information, see "OAuth 2.0 and OpenID Connect 1.0 Client Settings" in the *OAuth 2.0 Guide*.

  - **Improved Support for PKCE**

    In earlier versions of AM, the OAuth 2.0 Provider service could be configured to either require a PKCE code in all client requests, or to not require a code. This configuration was not very flexible for environments with both private clients and public clients.

    AM 6.5 allows configuring the OAuth 2.0 Provider service to specify which clients are required to present a PKCE code. To configure this feature, navigate to Realms > *Realm Name* > Services > OAuth2 Provider > Advanced, and select one of the following options in the Code Verifier Parameter Required drop-down field:

    - **All requests**. All clients must present a PKCE code.
    - **Requests from all public clients**. All public clients must present a PKCE code.
    - **Requests from all passwordless public clients**. All passwordless public clients must present a PKCE code.
    - **No requests**. No clients are required present a PCKE code.

  If a client makes a call to AM with the `code_challenge` parameter, AM will honor the code exchange regardless of the configuration of the Code Verifier Parameter Required field.

- Client-based Refresh Tokens are Now Whitelisted

  Client-based refresh tokens now have corresponding entries in a CTS whitelist, rather than a blacklist. When presenting a client-based refresh token AM will check that a matching entry is found in the CTS whitelist, and prevent reissue if the record does not exist.

Adding a client-based OAuth 2.0 token to the blacklist will also remove associated refresh tokens from the whitelist.

For more information on revoking client-based tokens, see "Configuring Client-Based OAuth 2.0 Token Blacklisting" in the *OAuth 2.0 Guide*.

# Security Advisories

ForgeRock issues security advisories in collaboration with our customers and the open source community to address any security vulnerabilities transparently and rapidly. ForgeRock's security advisory policy governs the process on how security issues are submitted, received, and evaluated as well as the timeline for the issuance of security advisories and patches.

For details of all the security advisories across ForgeRock products, see Security Advisories in the *Knowledge Base*.

Chapter 2

# Before You Install

This chapter covers software and hardware prerequisites for installing and running ForgeRock Access Management server software.

*ForgeRock supports customers using the versions specified here. Other versions and alternative environments might work as well. When opening a support ticket for an issue, however, make sure you can also reproduce the problem on a combination covered here.*

## Files to Download

Visit the ForgeRock Downloads Center for links to all available software downloads.

*AM Software*

| File | Description |
|---|---|
| `AM-6.5.5.zip` | Cross-platform distribution including all software components.<br><br>For a list of the files in the .zip archive, see "Obtaining Software" in the *Installation Guide*. |
| `AM-6.5.5.war` | Deployable web application archive file. |
| `SSOAdminTools-5.1.2.24.zip` | The .zip file that contains tools to manage AM from the command line. |
| `SSOConfiguratorTools-5.1.2.24.zip` | The .zip file that contains tools to configure AM from the command line. |

## Operating System Requirements

ForgeRock supports customers using ForgeRock Access Management server software on the following operating system versions:

*Supported Operating Systems*

| Operating System | Versions |
|---|---|
| Red Hat Enterprise Linux, Centos | 6, 7 |
| Amazon Linux | Amazon Linux 2 |

| Operating System | Versions |
|---|---|
| | Amazon Linux 2017.09<br>Amazon Linux 2018.03 |
| SuSE | 12 |
| Ubuntu | 14.04 LTS<br>16.04 LTS<br>18.04 LTS |
| Solaris x64 | 10, 11 |
| Solaris Sparc | 10, 11 |
| Windows Server | 2012 R2<br>2016 |

# Web and Java Agents Platform Requirements

The following table summarizes the minimum required version of web and Java agents:

*Minimum Agent Version Required*

| Agent | Versions |
|---|---|
| Web Agents | 5.0.1 |
| Java Agents | 5.0.1 |

AM supports several versions of web agents and Java agents. For supported container versions and other platform requirements related to agents, refer to the *ForgeRock Access Management Web Agents Release Notes* and the *ForgeRock Access Management Java Agents Release Notes*.

# Java Requirements

The following table lists supported Java versions:

*JDK Requirements*

| Vendor | Versions |
|---|---|
| Oracle JDK | 8, 11 [a] |
| IBM SDK, Java Technology Edition (WebSphere only) | 8 |
| OpenJDK | 8, 11 [a] |

[a]Federation-related pages do not display when using Java 11. For more information, see the Knowledge Base.

# Web Application Container Requirements

The following table summarizes supported application containers and their required versions:

*Web Containers*

| Web Container | Versions |
|---|---|
| Apache Tomcat | 7[a], 8.5, 9 |
| Oracle WebLogic Server | 12c (12.2.1.3) |
| JBoss Enterprise Application Platform | 7.1 |
| WildFly AS | 10.1, 11, 12 |
| IBM WebSphere | 8.5.5.8+[b], 9 |

[a]We recommend that you not use Apache Tomcat version 7.0.15+. We have found a bug where Tomcat throws a SocketTimeoutException when the application tries to read the request InputStream under high load. This issue affects Apache Tomcat 7.0.15+ and was fixed in version 8.5. For more information, see https://github.com/apache/tomcat80/pull/9.

[b]WebSphere 8.5.5.x does not have the required JEE libraries required to support WebSockets; therefore, this feature is impacted. Policy agents use this feature extensively and so would be impacted as well. WebSphere 9.x is not affected by this issue.

The web application container must be able to write to its own home directory, where AM stores configuration files.

**Caution**

Java Agents and Web Agents require the WebSocket protocol to communicate with AM.

Ensure that the container where AM runs, the web server/container where the agents run, and your network infrastructure all support the WebSocket protocol.

Refer to your network infrastructure and web server/container documentation for more information about WebSocket support.

# Directory Server Requirements

This section lists supported directory servers.

As described in "Generic LDAPv3 Configuration Properties" in the *Setup and Maintenance Guide*, you can configure AM to use LDAPv3-compliant directory servers as user data stores. If you have a special request to deploy AM with a user data store not mentioned in the following table, contact info@forgerock.com.

*Supported Directory Servers*

| Directory Server | Versions | Config | Apps/ Policies | CTS | Identities | UMA |
|---|---|---|---|---|---|---|
| Embedded ForgeRock Directory Services [a] | 6.5.6 | ✔ | ✔ | ✔ | ✔ | ✔ |
| External ForgeRock Directory Services | Any ForgeRock-supported version | ✔ | ✔ | ✔ | ✔ | ✔ |
| Oracle Unified Directory | 11g R2 | | | | ✔ | |
| Oracle Directory Server Enterprise Edition | 11g | | | | ✔ | |
| Microsoft Active Directory | 2012 R2, 2016 | | | | ✔ | |
| IBM Tivoli Directory Server | 6.3 | | | | ✔ | |

[a]Demo and test environments only

# Supported Clients

The following table summarizes supported clients and their minimum required versions:

*Supported Clients*

| Client Platform | Native Apps [a] | Chrome 62.0.3202[b] | Internet Explorer 11+[c] | Edge 25.10586 | Firefox 57+[b] | Safari 11[b] | Mobile Safari |
|---|---|---|---|---|---|---|---|
| Windows 8 | ✔ | ✔ | ✔ | | ✔ | | |
| Windows 10 | ✔ | ✔ | ✔ | ✔ | ✔ | | |
| Mac OS X 10.11 or later | ✔ | ✔ | | | ✔ | ✔ | |
| Ubuntu 14.04 LTS or later | ✔ | ✔ | | | ✔ | | |
| iOS 9 or later | ✔ | ✔ | | | | | ✔ |
| Android 6 or later | ✔ | ✔ | | | | | |

[a] *Native Apps* is a placeholder to indicate AM is not just a browser-based technology product. An example of a native app would be something written to use our REST APIs, such as the sample OAuth 2.0 Token Demo app.

[b]Chrome, Firefox, and Safari are configured to update automatically, so customers will typically be running latest. However, for RFP reasons, we specify a minimum version.

[c] Support for Internet Explorer 11 ends June 15, 2022, in alignment with the support announcement from Microsoft.

# Supported Upgrade Paths

The following table contains information about the supported upgrade paths to AM 6.5.5:

*Upgrade Paths*

| Version | Upgrade Supported? |
|---|---|
| AM 6.5.x | ✔ [a] |
| AM 6.0.x | ✔ [a] |
| AM 5.5 | ✔ |
| AM 5.0 (14.0) | ✔ |
| OpenAM 13.5.x | ✔ |
| OpenAM 13.x | ✔ |

[a]

[a] **Important**
The **Amster-config-upgrader** tool was removed from the AM 6.5.0 and later releases. As a result, after you upgrade your AM servers, you must manually export any Amster configuration files for them to be valid on the upgraded server. The Amster export applies to upgrades *to* AM 6.5.0, or from AM 6.5.0/6.5.0.x to AM 6.5.x (for example, AM 6.5.1 or 6.5.2). For more information, see How do I upgrade Amster configuration files when upgrading to AM 6.5.x or 7? in the *Knowledge Base*.

If you are upgrading from an unsupported version of AM to a later version, you must first upgrade to a supported version. In some cases, you may need to upgrade again depending on the upgrade path.

Upgrading between Enterprise and OEM versions is not supported.

For more information, see ForgeRock End of Service Life (EOSL) Policy and EOSL Dates in the *Knowledge Base*.

# Special Requests

If you have a special request regarding support for a combination not listed here, contact ForgeRock at info@forgerock.com.

Chapter 3

# Installing or Upgrading

This chapter covers installing and upgrading AM 6.5 software.

Before you install AM or upgrade your existing installation, read these release notes. Then, install or upgrade AM.

- If you are installing AM for the first time, see the Installation Guide.
- If you have already installed AM, see the Upgrade Guide.

Do *not* perform an upgrade by deploying the new version and then importing an existing configuration by running the **ssoadm import-svc-config** command. Importing an outdated configuration can result in a corrupted installation.

Chapter 4

# Changes and Deprecated Functionality

This chapter covers both major changes to existing functionality, and also deprecated and removed functionality.

## Critical Changes to Existing Functionality

As part of planning your upgrade, you need to consider that certain changes in later AM versions may have an impact on your environment. Usually, these changes are driven by changes in specification, security policies, or performance.

When possible, the upgrade process makes the appropriate changes on AM configuration. However, sometimes you will need to perform additional configuration based on your environment needs.

In addition to mandatory upgrade steps outlined in "*Upgrading AM Instances*" in the *Upgrade Guide*, if you are using features described in the following table you will need to perform additional upgrade tasks:

*Critical Changes to Existing Functionality*

| AM Version | Component or Feature | Change |
|---|---|---|
| 6.5.5 | Access to the API Explorer | For security reasons, access to the `/api` endpoint, and thus, to API Explorer, is now disabled by default. For instructions on enabling the API Explorer, see "Introducing the API Explorer" in the *Development Guide*. |
| | OAuth 2.0 Introspection Changes | HTTP GET requests are now disallowed on the `/oauth2/introspect` endpoint by default. Using `token` as a query parameter on this endpoint is also disallowed. To change this behavior to suit existing clients, use the `org.forgerock.openam.introspect.token.query.param.allowed` advanced server property. |
| 6.5.4 | Chain authentication `forceAuth` flag | In the chain authentication settings for both new and upgraded AM installations, the `ForceAuth` flag is enabled by default. This default setting will be incompatible with future AM versions, and may cause insecure behavior in some configurations.<br><br>If you are using authentication trees, or if you don't require ForceAuth to be enabled, then manually set `ForceAuth` to `false` now. In the Admin console, go to Configure > Server Defaults > |

| AM Version | Component or Feature | Change |
|---|---|---|
| | | Advanced. For details, see "Authentication Parameters" in the *Authentication and Single Sign-On Guide*. |
| | Splunk audit handler configuration | An authorization token in this configuration was stored in plain text in previous AM versions. Now the token is encrypted when saved. For added security, re-import and then re-export your Splunk configuration. |
| | Decompressed JWTs | By default, AM rejects any JWT that expands to more than 32 KiB (32768 bytes) when decompressed. For more information about changing this default, see "Controlling the Maximum Size of Compressed JWTs" in the *Installation Guide*. |
| | Request Body Size | By default, AM rejects incoming requests with a body larger than 1 MB (1048576 bytes) in size. For more information about changing this default value, see "Limiting the Size of the Request Body" in the *Installation Guide*. |
| | OAuth 2.0 and OpenID Connect Clients | This change affects AM when acting as an OAuth 2.0 or OpenID Connect client.<br><br>If a redirection URI uses a scheme, host, or port that differs from that of AM, add it to the Validation Service to ensure that it is pre-approved.<br><br>Otherwise, AM rejects the URI, and redirection fails. For more information, see "Configuring Success and Failure Redirection URLs" in the *Authentication and Single Sign-On Guide* |
| | The "Retry Limit Decision Node" in the *Authentication and Single Sign-On Guide* | The new Save Retry Limit to User feature in this node is disabled by default after upgrade. But, enabling this feature is strongly recommended and will require upgrading the identity store schema.<br><br>Ensure you update the schema following the instructions in "*Upgrading AM Instances*" in the *Upgrade Guide*, or disable the feature. ForgeRock recommends enabling this feature for security reasons. |
| 6.5.3 | OIDC ID token encryption | In 6.5.3, the OAuth 2.0 `idTokenEncryptionAlgorithm` setting determines how an OIDC ID token gets encrypted.<br><br>In 6.0.0x and earlier versions, the `com.forgerock.openam.oauth2provider.idTokenSignedResponseAlg` value in the OAuth 2.0 client administration endpoint determines how the OIDC ID token gets encrypted.<br><br>When you upgrade from 6.0 or earlier versions to 6.5.3 or later versions, entering an unsupported value for `idTokenEncryptionAlgorithm` may result in errors. For a list of supported values, see "ID Token Encryption Algorithms supported" under "OpenID Connect" in the *OAuth 2.0 Guide*. |

| AM Version | Component or Feature | Change |
|---|---|---|
| | `goto` and `gotoOnFail` Query Parameter Redirection | Redirection URLs for authentication services, agents, and SAML v.2.0 must be configured in the Validation Service if they are not in the same scheme, FQDN, and port as AM, or are not relative to AM's URL. |
| | `/json/authenticate` Endpoint | When a client makes a call to the `/json/authenticate` endpoint appending a valid SSO token, AM now returns the `tokenId` field **empty** when `HttpOnly` cookies are enabled. For example:<br>`{ "tokenId":"", "successUrl":"/openam/console", "realm":"/" }` |
| | SAML v2.0 Assertion Consumer Service | SAML v2.0 assertion consumer service URLs must exactly match the the SP's scheme, FQDN, and port. |
| | SAML v2.0 RelayState Redirection | To redirect to a domain outside of AM's deployment domain, you must add it to the Relay State URL List whitelisting property of the SP or IDP. |
| 6.5.0.2 and 6.5.1 | OAuth 2.0 Refresh Tokens | AM only issues refresh tokens to clients that have the `refresh token` grant type configured in their client profile.<br><br>After an upgrade to 6.5 or later using the UI or the **openam-upgrade-tool** .jar file, existing OAuth 2.0 clients are configured to use all grant flows, including the Refresh Token Grant flow.<br><br>To configure the `refresh token` grant type manually, see "To Configure AM to Issue Refresh Tokens" in the *OAuth 2.0 Guide*. |
| 6.5 | Recovery Codes | Recovery Codes are encrypted, and existing codes are no longer displayed to the user. For more information, see "Upgrading Device Recovery Codes" in the *Upgrade Guide*. |
| | Secret Stores | AM 6.5 introduced secret stores for OAuth 2.0 and the persistent cookie module. The upgrade process only creates the secret store files on the AM instance where you ran the upgrade process. For more information, see "Configuring Secret Stores After Upgrade" in the *Upgrade Guide*. |
| | External Configuration Store | DS 6.5 introduced setup profiles, which pre-configure instances for different usages, such as CTS or configuration data. The default base DN for a DS configuration store instance (`ou=am-config`) is different than the default used by previous versions of AM (`dc=openam,dc=forgerock,dc=org`).<br><br>You should not attempt to run multiple instances of AM where the configuration store base DNs do not match. Use the same configuration store base DNs when configuring external DS 6.5+ instances that will be used simultaneously alongside existing DS 6 or earlier configuration store instances. |

| AM Version | Component or Feature | Change |
|---|---|---|
| | | For more information, see "Preparing Configuration Stores" in the *Installation Guide*. |
| | Amster | The **Amster-config-upgrader** tool was removed. As a result, you need to upgrade AM following the procedures in the *Upgrade Guide* and then, export the configuration from the upgraded instance or site using Amster. For more information, see the following Knowledge Base article. |
| 6 | JSON Endpoints | AM's CSRF protection filter requires that either the `X-Requested-With` or the `Accept-API-Version` headers are included on requests to endpoints under the `json` root. For more information, see "Reviewing REST API Versions Before Upgrading" in the *Upgrade Guide*. |
| 5 | SSO Tokens | AM SSO session tokens are incompatible with SSO tokens from OpenAM.<br><br>CTS-based (stateful) and client-based (stateless) sessions created by earlier versions of OpenAM are not supported. After upgrading from an earlier version, any existing SSO tokens created by that version will become invalid, and users will need to reauthenticate. In mixed version deployments, earlier versions of OpenAM will not be able to read or process SSO session tokens created by AM 5 or later.<br><br>This incompatibility only affects SSO session tokens. OAuth 2.0 and OpenID Connect 1.0 tokens are interoperable between versions. |
| | Realms | Realm paths now must be absolute and include the top-level realm, and DNS aliases and realms specified in the query string are no longer concatenated if used together – the query string overrides the DNS alias.<br><br>For examples, see "Specifying the Realm in the Login URL" and "Specifying Realms in REST API Calls" in the *Authentication and Single Sign-On Guide*.<br><br>This change also impacts the user self-service feature when deployed in subrealms. For more information, see "Upgrading User Self-Service in Subrealms" in the *Upgrade Guide*. |
| | Post-Authentication Plugins | AM does not maintain state in post-authentication plugins between login and logout anymore. For more information, see "Upgrading Post-Authentication Plugins" in the *Upgrade Guide*. |
| 13.5 | User Self-Service | The user self-service feature requires two keys in a JCEKS keystore. For more information, see "Upgrading the Keystore for User Self-Service" in the *Upgrade Guide*. |

# Important Changes to Existing Functionality

This section lists changes made to existing functionality, services, endpoints, and others in the current release of AM.

## *AM 6.5.5*

- Changes in Base URL `X-Forwarded-*` headers
  - Previously, if you set the Base URL Source to `X-Forwarded-* headers` and no `X-Forwarded-Proto` header was provided, the generated URL would have a protocol of `null`, for example `null://host`, which would result in a broken URL.

    From this release, if no `X-Forwarded-Proto` header is provided, a fallback scheme is used, based on the URI of the request.
  - You can now specify a port in the Base URL, using the `X-Forwarded-Port` header.
  - If multiple `X-Forwarded-Host` headers are specified, the outermost proxy host is used.
- Number of Connections Made by the CTS

  OPENAM-13855 corrected an issue where the CTS was creating too many connections to the Directory Services. This fix might imply that the number of connections created is now different in your deployment, corrected to be the expected number of connections. Monitor your environments to ensure that this corrected number of connections is sufficient, and increase it if necessary.

## *AM 6.5.4*

- Maximum Size of Decompressed JWTs Enforced

  A number of AM features accept JWTs to receive information. Some examples are:

  - The Remote Consent service, when it receives consent responses.
  - The OAuth 2.0/OpenID Connect authorization service, when:
    - OpenID Connect clients send `request` parameters as an encrypted JWT instead of as HTTP parameters.
    - OpenID Connect clients register dynamically using software statements.
  - The Authentication service, when configured to issue client-based sessions.

  These JWTs that AM receives can be signed and/or encrypted. Sometimes, if they are fairly large, they can also be compressed so that requests reach AM faster.

  Decompressing a JWT makes it expand in size. By default, AM 6.5.4 rejects any JWT that expands to more than 32 KiB (32768 bytes).

Before upgrade, ensure that the decompressed JWTs your clients send to AM are smaller than 32 KiB before compression. If not, change the default value to a larger number after upgrade.

For more information about changing the default value, see "Controlling the Maximum Size of Compressed JWTs" in the *Installation Guide*.

- Changes to the OAuth 2.0 and OpenID Connect Clients

  AM 6.5.4 returns an error if the administrator tries to save a client configuration containing an unsupported signing or encryption algorithm.

  For example, upon saving the configuration, AM will return an error if there is a typo on an algorithm, or a symmetric signing or encryption algorithm is configured on a public client: these algorithms are derived from the client's secret, which public clients do not have.

  Clients registering dynamically must also send supported algorithms as part of their configuration, or AM will reject the registration request.

  Different features support different algorithms. Refer to the documentation or to the UI for more information.

  The following are examples of the errors:

  - `Unknown encryption algorithm configured for User info encrypted response algorithm`
  - `Symmetric encryption algorithm configured for ID Token Encryption Algorithm is not allowed for a public client`

  The error messages are also logged at ERROR level, and identify the client ID that the error relates to.

- The OpenID Connect Discovery Endpoint is Now Disabled by Default

  The `/.well-known/webfinger` OpenID Connect discovery endpoint is now disabled by default, and can only be enabled by realm.

  To enable the endpoint for a realm, configure the OAuth2 Provider service on the realm and next, enable the new OIDC Provider Discovery switch. Enabling the endpoint for the realm allows searches for users within that realm only.

  After upgrading to AM 6.5.4, the endpoint will be enabled on realms that had the OAuth2 Provider service configured. Disable the endpoint on those realms that are not using OpenID Connect discovery.

  For more information about the endpoint, see "Configuring AM for OpenID Connect Discovery" in the *OpenID Connect 1.0 Guide*.

- Maximum Size of Request Body Enforced

Application servers can usually mitigate against DoS attacks that POST large amounts of form data, but AM endpoints may receive large amounts of POST data in different ways, such as in JSON, JWT, or JWK formats.

By default, AM 6.5.4 rejects incoming requests with a body larger than 1 MB (1048576 bytes) in size, and returns an HTTP 413 error response.

For more information about changing the default value, see "Limiting the Size of the Request Body" in the *Installation Guide*.

- Changes to the OAuth 2.0 Introspection Response

  The `/oauth2/introspect` endpoint now returns an additional member, `username`, which specifies the user that authorized the introspected token.

  As part of this change, the `user_id` member, which was used by earlier versions of the specification, is deprecated. It will be removed in a future version of AM.

  This change aligns the endpoint's response with the OAuth 2.0 Token Introspection specification.

- Changes to the `expires_in` Value Returned from OAuth 2.0 Endpoints

  AM 6.5.4 changes the way the `/oauth2/introspect` and the `/oauth2/tokeninfo` endpoints return the value of the `expires_in` object.

  The `expires_in` object specifies the time, in seconds, that a token is valid for. For example, 3600 seconds. This value is set at token creation time, and it depends on the configuration of the OAuth2 Provider Service.

  When providing a token introspection or token information response, earlier versions of AM returned the value of the `expires_in` object as it was stored in the token. This means that any call to the endpoints while the token is valid returned the same value for the `expires_in` object.

  AM 6.5.4 calculates the amount of seconds the token is still valid for and returns this value in the `expires_in` object. Therefore, repeated calls to the endpoints return different values for the object.

  However, the actual value of the `expires_in` object in the token does not change. Inspecting the token without using AM will show the value set at token creation time.

  **Note**

  The `expires_in` object is not always present in the endpoint response:

  **Introspection endpoint**: AM *only* returns the `expires_in` object for client-based tokens issued to a client configured in the same realm as the resource owner's.

**Token information endpoint**: AM does not return the `expires_in` object for client-based tokens issued to a client configured in a different realm than the resource owner's.

- Changes to the Values Returned From the OpenID Connect User Information Endpoint

  AM 6.5.4 changes when the `aud` and `iss` objects are returned in the JWT response of the `/oauth2/userinfo` endpoint.

  Earlier versions of AM returned the `iss` object when the user information response was a signed, encrypted, or a signed and encrypted JWT. The `aud` object was never returned.

  AM 6.5.4 now returns both the `aud` and `iss` objects when response is a signed, or a signed and encrypted JWT, according to the OpenID Connect Core 1.0 incorporating errata set 1 specification.

  The `iss` object is no longer returned when the response is an encrypted JWT.

- One-Time Passwords Are Now Encrypted in the Authentication Tree's Shared State

  New installations of AM 6.5.4 now encrypt one-time passwords (OTPs) created by the HOTP Generator Node because the passwords are stored in the authentication tree's shared state.

  As a security measure, when you upgrade to AM 6.5.4, OTP encryption is enabled by default. This will impact any existing scripts that use the `oneTimePassword` property in the shared state.

  OTP encryption in the shared state is dependent on the following configuration:

  - Mapping a secret to the `am.authn.nodes.sharedstate.encryption` secret ID, which has been added for this purpose.
  - Enabling the new `org.forgerock.am.auth.node.otp.encrypted` advanced server property.

  To let the Scripted Decision Node retrieve and work with encrypted one-time passwords, AM 6.5.4 includes the new `org.forgerock.openam.auth.nodes.crypto.NodeSharedStateCrypto` Java class and its scripting binding, `sharedStateCrypto`.

  The class is whitelisted in the scripting engine by default in new installations of AM 6.5.4, and after upgrading.

  Use the `sharedStateCrypto` binding to encrypt or decrypt the one-time password and one-time password timestamp, if needed. For more information, see "Encrypting and Decrypting Shared State Data" in the *Authentication and Single Sign-On Guide*.

  **Important**

  Use of the `sharedStateCrypto` object is intended to encrypt and decrypt one-time passwords along with their timestamps in the *Authentication and Single Sign-On Guide* only.

The `org.forgerock.openam.auth.nodes.crypto.NodeSharedStateCrypto` Java class included in AM 6.5.4 or later and its `sharedStateCrypto` scripting binding do not exist in AM 7 or later because `org.forgerock.openam.auth.nodes.crypto.NodeSharedStateCrypto` no longer exists.

Any scripts or authentication nodes using this class and/or binding will need to be updated accordingly when upgrading to AM 7 or later because `org.forgerock.openam.auth.nodes.crypto.NodeSharedStateCrypto` no longer exists.

### *Important Changes in AM 6.5.3*

- Clarification on Retrieving User Attributes from a Session Using the REST API

  When retrieving user attributes from a session using REST, use of the `User Attribute Mapping to Session Attribute` and `Whitelisted Session Property Names` properties only apply to authentication modules in pre-AM 6.5.3 versions, and to authentication trees and modules in AM 6.5.3 and later versions.

  For additional information, see How do I retrieve user attributes from a session using the REST API in AM (All versions) and OpenAM 13.5? on the *ForgeRock Knowledge Base*.

- Support for Encrypted ID Tokens Added to the OpenID Connect End Session Endpoint

  In earlier versions of AM, trying to end a session using an encrypted ID token resulted in failure, since the request did not include enough information for AM to decrypt the token.

  To support ending sessions when ID tokens are encrypted, AM 6.5.3 requires that the request to the end session endpoint includes the client ID for which AM issued the ID token.

  This change diverges from the specification defined in the OpenID Connect Session Management 1.0-draft 5.

  For more information, see "/oauth2/connect/checkSession" in the *OpenID Connect 1.0 Guide*.

- LDAP Connection Pool Property Name Corrected

  The `com.sun.am.ldap.connection.idle.seconds` property has been corrected. If you have any files or scripts which have the previous spelling, `com.sun.am.ldap.connnection.idle.seconds`, you should correct them to the new, correct spelling.

  For more information about this property, see "Tuning LDAP Connectivity" in the *Setup and Maintenance Guide*.

- Removed Default Value of the Json Web Key URI Field for OAuth 2.0/OpenID Connect Clients

  When creating a new OAuth 2.0 or OpenID Connect client, earlier versions of AM set the value of the Json Web Key URI field to the `jwk_uri` endpoint in AM. For example, `https://openam.example.com:8443/openam/oauth2/connect/jwk_uri`.

The value of the Json Web Key URI field in the client should not be AM's `jwk_uri` endpoint, but an external URL holding the client's public JWK.

New clients created in AM 6.5.3 will have this field empty to avoid confusion, but existing clients will not be modified after upgrade.

- Service Configuration Notifications Processed Sequentially by Default

  The `com.sun.identity.sm.notification.threadpool.size` property now defaults to `1`, which causes notifications to be processed sequentially, avoiding any potential out-of-order conditions.

  For more information about this property, see "Notification Settings" in the *Setup and Maintenance Guide*.

- WDSSO: Absolute Path of Keytab File Must Be Specified

  When configuring Windows Desktop SSO (WDSSO), the absolute path of the keytab file must be specified, instead of the URL. On the AM UI console, navigate to Authentication > Modules > Windows Desktop SSO, click the Info icon next to the Keytab File Name field for information.

- Changes to the Audit Logging Service

  AM 6.5 introduced the `AM-IDENTITY-CHANGE` and `AM-GROUP-CHANGE` audit events to log user and group-related changes our updates such as password changes, user creation and deletion, and others.

  AM 6.5.3 does not log this information by default, since doing so may have a performance impact on the AM instances.

  To configure whether the Audit Logging Service should log these events, AM 6.5.3 includes the `org.forgerock.openam.audit.identity.activity.events.blacklist` advanced server property, which also enables and disables the logging of `AM-ACCESS-ATTEMPT` events.

  This property replaces the `org.forgerock.openam.audit.access.attempt.enabled` advanced server property, which has been removed.

  For more information, see "Advanced Properties" in the *Reference*.

- Changes to the User Self-Service Flows

  AM 6.5.3 no longer reports if an account does not exist while recovering a username or password, or if an account already exists when registering a new one:

  - Recovery Flows

    When KBA or email are enabled as security methods, the flow will not stop when the user introduces the invalid username. Instead, AM does one of the following, depending on which security method is configured:

    - Presents the user with a random KBA question before failing.

- Presents the user with a message similar to `An email has been sent to the address you entered. Click the link in that email to proceed`, but does not actually send an email.

If both methods are configured, then AM presents the user with the email message.

- Registration Flow

When email is enabled as a security method, AM presents the user with a message similar to `An email has been sent to the address you entered. Click the link in that email to proceed`, and then sends an email with a registration link to the address that the user entered.

Clicking on the link sends the user to the registration page again, and AM shows a message similar to `One or more user account values are invalid`.

- `alg` Parameter Removed from Keys Returned by JWK URI Endpoints

AM 6.5.3 removes the `alg` parameter from the keys returned by the JWK URI endpoints. As a result, each `kid` is now unique.

- Changes to the `goto` and `gotoOnFail` Redirections

Earlier versions of AM redirected the user to the URL specified in the `goto` and `gotoOnFail` query string parameters supplied to the authentication service, SAML v2.0 entities, or agents during login and logout. To harden security against phishing attacks, we recommended that you configure the Validation Service.

By default, AM 6.5.3 only redirects to the URLs specified in those query string parameters if the URLs are in the same scheme, FQDN, and port as AM, or to URLs relative to AM. You *must* configure any other URL in the Validation Service.

+ *Do I Need to Add my URL to the Validation Service?*

Consider an example AM deployment configured in `https://openam.example.com:8443/openam`:

| URL | Needs to be configured in the Validation Service? |
|---|---|
| `http://openam.example.com:8080/openam/XUI/#login` | Yes, the scheme and port are different. |
| `https://openam.example.com:443/openam/XUI/#login` | Yes, the port is different. |
| `/openam/XUI/#login` | No, the paths relative to the AM URL are trusted. |
| `https://mypage.example.com/app/logout.jsp` | Yes, the scheme, port, and FQDN are different. |

For more information, "Configuring Success and Failure Redirection URLs" in the *Authentication and Single Sign-On Guide*.

- SSO Token Not Returned When Authentication Endpoint Called with an Existing Session and `HttpOnly` Cookies Are Enabled

  When a client appends a valid SSO token to a call to the `/json/authenticate` endpoint, earlier versions of AM return the SSO token again in the `tokenId`field of the JSON response, regardless of the flags configured for the session cookie. For example:

  ```
  {
      "tokenId":"AQIC5wM2...",
      "successUrl":"/openam/console",
      "realm":"/"
  }
  ```

  AM 6.5.3 now returns the `tokenId` field **empty** when `HttpOnly` cookies are enabled. For example:

  ```
  {
      "tokenId":"",
      "successUrl":"/openam/console",
      "realm":"/"
  }
  ```

  Remember that AM upgrades cookies to secure cookies (except the `amlbcookie` cookie) when requests arrive over a secure channel.

  To check if `HttpOnly` session cookies are configured, see "Configuring HttpOnly" in the *Authentication and Single Sign-On Guide*.

  Change any custom login pages or applications that were expecting the old response, for example, for session upgrade cases.

- SAML v2.0 Assertion Consumer Service URLs Must Exactly Match

  When AM acts as the hosted service provider, the scheme, FQDN, and port of the URLs specified in the Assertion Consumer Service must exactly match those of the service provider as they appear in its metadata.

  To determine the service provider's endpoint URL, AM uses the Base URL service, if configured.

  If the URL does not match, the SAML v2.0 flow will fail and AM will log `Invalid Assertion Consumer Location specified` in the audit log file.

- SAML v2.0 RelayState Redirection Restricted to Same Domain as the AM Instance

  AM 6.5.3 alters the behavior of the Relay State URL List whitelisting property. If you do not specify any URLs in this property, AM will only redirect to URLs that match its deployment domain; for example, `example.com`.

  To be able to redirect using the RelayState parameter to a URL that does not match the instance of AM, you **MUST** add the URL to the Relay State URL List property.

  For more information, see Relay State URL List - Hosted IDP or Relay State URL List - Hosted SP in the *SAML v2.0 Guide*

### *Important Changes in AM 6.5.2.3*

- Please see Improvements in AM 6.5.2.3.

### *Important Changes in AM 6.5.2.2*

- There are no important changes in functionality in this release.

### *Important Changes in AM 6.5.2.1*

- There are no important changes in functionality in this release.

### *Important Changes in AM 6.5.2*

- Trusted JWT Issuer on Admin Console under Agents Menu

  The location of the Trusted JWT Issuer is located under the Agents menu on the Admin Console. You can access it by navigating to Applications > Agents > Trusted JWT Issuer.

  **Note**

  In AM version 7.x, Trusted JWT Issuer will be located at Applications > OAuth 2.0 > Trusted JWT Issuer.

- Added Key Transport Algorithm Setting

  AM 6.5.2 introduces a new Key Transport Algorithm setting for SAML v2.0 remote and hosted IdPs and SPs, attribute authorities, and attribute query entity roles.

  The key transport algorithm is used to encrypt the symmetric encryption key when SAML v2.0 token encryption is enabled.

  Consider an example where the IdP starts a SAML v2.0 flow. Simplifying, the IdP creates a SAML v2.0 assertion and a symmetric key, and encrypts the assertion with it. Then, using the SP's public client certificate and the SP's advertised transport key algorithm, the IdP encrypts the symmetric key.

  Finally, the IdP sends both the encrypted assertion and the encrypted symmetric key to the SP, which decrypts both to continue the flow.

  Therefore, if you want a hosted provider to use a specific transport key algorithm, you must configure the remote provider to advertise it.

  Remote and hosted IdPs and SPs, attribute authorities, and attribute query entity roles support the following transport key algorithms:

  - http://www.w3.org/2001/04/xmlenc#rsa-1_5.

Earlier versions of AM only supported RSA v1.5, which was preconfigured for the entities and could not be changed.

For security reasons, we recommend that you no longer use this algorithm.

- http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p (default).
- http://www.w3.org/2009/xmlenc11#rsa-oaep.

When this algorithm is configured, AM will use the Mask Generation Function Algorithm property (Configure > Global Services > Common Federation Configuration) to create the transport key.

For a list of supported mask generation function algorithms, see "Algorithms" in the *Reference*.

The Key Transport Algorithm field *is not editable* for remote providers. Update the remote provider's metadata with the new algorithm and reimport it, instead.

This change also updates the STS service, adding a Key Transport Algorithm field under Realms > *Realm Name* > STS > *STS Name* > SAML2 Token.

- Authentication Nodes Now Can Access `HttpServletRequest` and `HttpServletResponse` available from `ExternalRequestContext`

  Authentication nodes now have access to `HttpServletRequest` and `HttpServletResponse`, which is available from `ExternalRequestContext`.

### *Important Changes in AM 6.5.1*

- Change to OAuth 2.0 Client Issuance of a Refresh Token

  **Important**

  For OAuth 2.0 clients, the `refresh_token` grant type must now be provided to obtain a refresh token. In previous AM versions, the OAuth 2.0 client would issue both an access and refresh token, even if the refresh token flow was not enabled on the client.

  This has been changed in AM 6.5.1 to be more compliant with the specification.

  The client will need to have the refresh token configured as a grant type to abe to receive and use the refresh token. For more information, see "To Configure AM to Issue Refresh Tokens" in the *OAuth 2.0 Guide*.

- LDAPv3Repos LDAP Servers are Now Stored in Comma-Separated Ordered List

  For multiple data stores behind a load balancer deployment, AM now stores its servers as a comma-separated list, rather than an ordered list.

  For example, given a site configuration, ID 02, with two servers, IDs 01 and 03. In previous releases (prior to AM 6.5.1), AM would store the servers as an ordered list:

```
$./ldapsearch -p 51389 -D "cn=Directory Manager" -w cangetin -b
 "ou=services,dc=openam,dc=forgerock,dc=org" "objectclass=*"  > backup.ldif
$ grep "sun-idrepo-ldapv3-config-ldap-server" backup.ldif
sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=xxx.example.com:1389|01|02
sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=zzz.example.com:1389|01|02
sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=xxx.example.com:1389|03|02
sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=localhost:51389
sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=zzz.example.com:1389|03|02
```

Now, AM stores its multi-server configuration as a comma-separated ordered list:

```
$./ldapsearch -p 51389 -D "cn=Directory Manager" -w cangetin -b
 "ou=services,dc=openam,dc=forgerock,dc=org" "objectclass=*"  > backup.ldif
$ grep "sun-idrepo-ldapv3-config-ldap-server" backup.ldif
sunKeyValue: sun-idrepo-ldapv3-config-ldap-server=[0]=xxx.example.com:1389|01|02,xxx.example.com:1389|
03|02,localhost:51389,zzz.example.com:1389|01|02,zzz.example.com:1389|03|02
```

- `request_uri` Values Must Be Pre-Registered

  In earlier versions of AM, you could configure the OAuth 2.0/OpenID Connect provider to require clients to pre-register their `request_uri` values.

  Now, pre-registration of `request_URI` values is mandatory, and the option to disable it has been removed.

- Added Support for the `none` Authentication Method for OpenID Connect Clients

  In earlier versions of AM, public OpenID Connect clients could not specify the `none` authentication method when registering.

  AM 6.5.1 adds the `none` authentication method for OpenID Connect clients, as per RFC7591.

### *Important Changes in AM 6.5.0.2*

- Change to OAuth 2.0 Client Issuance of a Refresh Token

  **Important**

  For OAuth 2.0 clients, the `refresh_token` grant type must now be provided to obtain a refresh token. In previous AM versions, the OAuth 2.0 client would issue both an access and refresh token, even if the refresh token flow was not enabled on the client.

  This has been changed in AM 6.5.0.2 to be more compliant with the specification.

  The client will need to have the refresh token configured as a grant type to abe to receive and use the refresh token. For more information, see "To Configure AM to Issue Refresh Tokens" in the *OAuth 2.0 Guide*.

- Updated Versions of the Admin Tools and Configurator Tools Utilities

  AM 6.5.0.2 also includes an updated version of the Admin Tools (`AM-SSOAdminTools-5.1.2.3.zip`) and the Configurator Tools (`AM-SSOConfiguratorTools-5.1.2.3.zip`) utilities. These upgraded versions of

the tools fixes an issue that could cause the **ssoadm** to malfunction while using JDK 11 or JDK 1.8.0_192+ (see Known Issues in AM 6.5). You can download these versions from the *ForgeRock Backstage* website.

### *Important Changes in AM 6.5.0.1*

- There are no important changes in AM 6.5.0.1, other than those identified in Important Changes in AM 6.5.

### *Important Changes in AM 6.5*

- Web and Java Agents Earlier than 5.0.1 Not Supported

  AM 6.5 does not interoperate with web and Java agents earlier than 5.0.1.

- Stored Device Recovery Codes are now One-way Encrypted

  AM 6.5 encrypts stored device recovery codes by default. This means they can only be shown to users a single time before they become encrypted, and therefore, unreadable.

  **Important**

  To prevent AM from encrypting existing device recovery codes you must add a Java property to your environment, BEFORE starting the container.

  For more information on device recovery code encryption, and how to disable encryption, see "To Prevent AM Encrypting Device Recovery Codes" in the *Upgrade Guide*.

- **Utils Class Containing SHA-1 Usage Moved**

  The class `org.forgerock.oauth2.core.Utils#getKid` has moved to `org.forgerock.openam.secrets.SecretsUtils#getStaticId` in AM 6.5.

  This class may get flagged for SHA-1 usage in source code scans. However, reports of this particular use of SHA-1 can be safely ignored.

  For more information, see Security scan shows use of SHA-1 in Utils class in AM/OpenAM (All versions) in the *Knowledge Base*.

- **Naming Convention Changes on Documentation and UI**

  Earlier versions of the AM documentation and the UI classify OAuth 2.0 and OpenID Connect 1.0 tokens as *stateful* when AM stores tokens in the CTS token store, and *stateless* when AM returns the token to the client.

  This naming convention is misleading. OAuth 2.0 services are stateless (no information regarding OAuth 2.0 is stored in the AM server memory), and any server in the AM deployment can satisfy any OAuth 2.0-related request.

AM 6.5 removes the stateful/stateless naming convention and classifies tokens depending on where they are stored:

- CTS-based tokens (previously referred to as stateful tokens)
- Client-based tokens (previously referred to as stateless tokens)

- Signing Methods for Social Authentication with IDM Incompatible with Earlier Versions

  The signing method used by AM 6.5 when performing social authentication with IDM 6.5 has changed, in order to support non-extractable HMAC keys from Hardware Security Modules (HSMs).

  The new signing method is not compatible with IDM 6, or earlier.

  If you have not upgraded to IDM 6.5, or later, enable the new Signing Compatibility Mode property in the IDM Provisioning service in order to use social authentication involving IDM successfully.

  For more information, see "IDM Provisioning" in the *User Self-Service Guide*.

- The Amster Configuration Upgrader Utility is not Included in the AM 6.5 Release

  The tool is used to upgrade configuration files exported by Amster for use in later versions.

*Upgrade Paths*

| Version | Upgrade To | Manual Amster Export ? |
|---|---|---|
| AM 6.0.0.x | AM 6.5.x | ✔ |

  Follow the procedures in the Upgrade Guide to upgrade from previous versions to AM 6.5. Then, use Amster to export configuration files that are compatible with AM 6.5.

- Data Stores Renamed to Identity Stores

  To differentiate the stores used for identities from those used for configuration, applications, or policies, the *Data Stores* label in the user interface has been renamed to *Identity Stores*.

- Changes to the Prometheus Monitoring Interface

  In earlier versions of AM, Prometheus had to authenticate with a username and a password when accessing the monitoring endpoint. AM 6.5 allows you to configure the monitoring interface such that Prometheus can access the endpoint without authenticating.

  For more information, see "Prometheus Monitoring" in the *Setup and Maintenance Guide*.

- Oracle WebLogic Required Packages Now Included by Default

  In earlier versions of AM, Bouncy Castle and Jackson packages needed to be added to the `weblogic.xml` file in order to deploy AM successfully in Oracle WebLogic.

This step is no longer required, as the packages are included by default.

For more information, see"Preparing Oracle WebLogic" in the *Installation Guide*.

- Changes to the activity.audit.json Log File

  In earlier versions of AM, the activity.audit.json log file only captured session changes. AM 6.5 captures session, user profile, and device profile changes in the logs.

  For more information, see "Audit Log Topics" in the *Setup and Maintenance Guide*.

- UI Source Paths Changed

  In earlier versions of AM, the source code of the UI pages was under `openam-ui-ria/src/main`. AM 6.5 removes the `main` directory.

  For more information about the new paths, see "Customizing the XUI" in the *UI Customization Guide*.

- Default com.sun.identity.sm.sms_object_class_name Changed

  In earlier versions of AM, the default com.sun.identity.sm.sms_object_class_name was `com.sun.identity.sm.ldap.SMSEmbeddedLdapObject`. AM 6.5 updates the default to be `com.sun.identity.sm.SmsWrapperObject`.

  For more information, see "Advanced Properties" in the *Reference*

# Deprecated Functionality

Functionality listed under this section has been deprecated and will be removed in a future release of AM.

### *Deprecated Functionality in AM 6.5.4*

- Deprecated Existing `getIDPAuthnContextInfo` Signature

  The existing signature for the `getIDPAuthnContextInfo` method of the `IDPAuthnContextMapper` interface is deprecated.

  AM 6.5.4 includes a new signature for the getIDPAuthnContextInfo method, which includes an additional parameter for the entity ID of the service provider (SP).

  Note that the deprecated method still works in AM 6.5.4, but you should update any code that uses it to the new four-parameter signature. The deprecated three-parameter signature will be removed in a future version of AM.

- The `user_id` Member in the OAuth 2.0 Introspection Response is Deprecated

The `user_id` member, which is part of the JSON response returned by the `/oauth2/introspect` endpoint, is deprecated. It will be removed in a future release of AM.

### *Deprecated Functionality in AM 6.5.3*

- Support for installing AM in Oracle WebLogic Server is deprecated, and will be removed in a later release.

### *Deprecated Functionality in AM 6.5.2.3*

- No functionality has been deprecated in this release, other than those identified in Deprecated Functionality in AM 6.5.2.1 and Deprecated Functionality in AM 6.5.

### *Deprecated Functionality in AM 6.5.2.2*

- No functionality has been deprecated in this release, other than those identified in Deprecated Functionality in AM 6.5.2.1 and Deprecated Functionality in AM 6.5.

### *Deprecated Functionality in AM 6.5.2.1*

- The Windows NT authentication module was deprecated in this release.

### *Deprecated Functionality in AM 6.5.2*

- No functionality has been deprecated in this release, other than those identified in Deprecated Functionality in AM 6.5.

### *Deprecated Functionality in AM 6.5.1*

- No functionality has been deprecated in this release, other than those identified in Deprecated Functionality in AM 6.5.

### *Deprecated Functionality in AM 6.5.0.2*

- No functionality has been deprecated in this release, other than those identified in Deprecated Functionality in AM 6.5.

### *Deprecated Functionality in AM 6.5.0.1*

- No functionality has been deprecated in this release, other than those identified in Deprecated Functionality in AM 6.5.

### *Deprecated Functionality in AM 6.5*

- **SAML 1.0 Deprecated**

SAML 1.0 functionality is deprecated in AM 6.5, and will be removed in a future version.

- The ssoadm, ampassword, configurator.jar and upgrade.jar Tools Remain Deprecated

  The **ssoadm** command and the `configurator.jar`, `upgrade.jar`, and `ampassword` tools remain deprecated. They will be removed in a future release of AM.

# Removed Functionality

Functionality listed under this section has been removed from AM.

### *Removed Functionality in AM 6.5.4*

- Access to the legacy `/identity` endpoints has been removed.

### *Removed Functionality in AM 6.5.3*

- Removed the `org.forgerock.openam.audit.access.attempt.enabled` Advanced Server Property

  It has been replaced with the `org.forgerock.openam.audit.identity.activity.events.blacklist` advanced server property.

  For more information, see "Advanced Properties" in the *Reference*.

### *Removed Functionality in AM 6.5.2.3*

- No features or functionality have been removed in this release.

### *Removed Functionality in AM 6.5.2.2*

- No features or functionality have been removed in this release.

### *Removed Functionality in AM 6.5.2.1*

- No features or functionality have been removed in this release.

### *Removed Functionality in AM 6.5.2*

- No features or functionality have been removed in this release.

### *Removed Functionality in AM 6.5.1*

- No features or functionality have been removed in this release.

### *Removed Functionality in AM 6.5.0.2*

- No features or functionality have been removed in this release.

### *Removed Functionality in AM 6.5.0.1*

- No features or functionality have been removed in this release.

### *Removed Functionality in AM 6.5*

- No features or functionality have been removed in this release.

Chapter 5

# Fixes, Limitations, and Known Issues

This chapter covers the status of key issues and limitations at release 6.5.

## Fixed Issues

The following important bugs were fixed in this release:

*Key Fixes in AM 6.5.5*

- OPENAM-12101: Connection pool not restarted if LDAP authentication module admin bind password is incorrect
- OPENAM-12992: Misleading error message in XUI console for existing DNS alias
- OPENAM-13312: Stateless non-expiring refresh tokens fail with "invalid_grant"
- OPENAM-13855: CTS creates too many connections to DS
- OPENAM-13912: Node implementations are loading the resource bundles incorrectly
- OPENAM-14343: AM console - localization issue for algorithms in global Common Federation Configuration
- OPENAM-15408: `oauth2/connect/jwk_uri` does not expose keys of the remote consent agent profile
- OPENAM-15472: HOTP - text for performed attempts is hard-coded and not localisable
- OPENAM-15682: AM jwks_uri doesn't reflect changes to secret mappings
- OPENAM-16490: OWASP ESAPI lib is missing some classes
- OPENAM-17593: Deadlock when admin token is invalid and when config data is cleared
- OPENAM-17882: Slow memory leaks when persistent search starts a retry activity when persistent search fails
- OPENAM-17904: JSON Audit Log Location not working when modifying location to only include `%SERVER_URI%` variable

- OPENAM-17962: LDAP Decision Node does not put updated password in transient state
- OPENAM-18005: Insufficient error message to troubleshoot persistent search issue
- OPENAM-18006: Persistent search for identity store does not recover when re-configuring identity store
- OPENAM-18030: Message node shows inconsistent behavior regarding the default locale
- OPENAM-18062: `SPACSUtils` withholds exception and does not log error
- OPENAM-18090: Creation of UMA Policy to share a resource fails when identities have custom attributes
- OPENAM-18113: LDAP auth node - change of connection mode does not re-created connection pool
- OPENAM-18121: Complex authentication trees load slowly
- OPENAM-18140: AM Error "Trying to redefine version 0.0 for path" thrown on AM startup with forgeops
- OPENAM-18268: `webauthnDeviceProfiles` is not multi-valued for AD
- OPENAM-18306: OAuth2 Authorization Code Grant Fails when including scope parameter at access_token endpoint
- OPENAM-18359: Choice Collector Node not present following upgrade
- OPENAM-18372: After upgrade from 5.1.1 to 6.5.4 Mail server secure connection value is displayed incorrectly in XUI
- OPENAM-18377: Authorization fails using auth module if user has authenticated with alias name
- OPENAM-18477: Choice Collector Callback fails to replaceSharedState() using Action.send() method inside Page Node
- OPENAM-18573: URLPatternMatcher or RedirectURLValidator fails when query string contains "%20"
- OPENAM-18586: No debug message when AM can't read the encrypted_base64 folder after upgrade
- OPENAM-18610: RealmOAuth2ProviderSettings for `getJwks` permits an empty set
- OPENAM-18655: Deleting OAuth2 Client causes unnecessary notification error message in IdRepo
- OPENAM-18679: OATH Registration node doesn't work when placed inside a 'Page' node
- OPENAM-18753: Upgrading AM Radius server with clients causes Radius auth failures
- OPENAM-18756: Entering correct OTP after an incorrect OTP fails authentication

- OPENAM-18833: Client authentication using private_key_jwt will cause 500 if claims value is null
- OPENAM-18864: Upgrade Radius Server Client Secrets fails due to service config cache cleared
- OPENAM-18883: Inconsistent error response from Client authentication using private_key_jwt
- OPENAM-18921: Double slashes in oauth2 claim name handled incorrectly
- OPENAM-18928: Client credential OAuth2 request results in searches for OAuth2 client against Identity Store
- OPENAM-18990: Non-compliant OAuth2 error response generated
- OPENAM-19083: Creating a client-based access & refresh token breaks subsequent use of Session Quotas
- OPENAM-19108: "Agent" auth tree creates tokens with insufficient permissions
- OPENAM-19111: Insufficient debug logging to troubleshoot error "Illegal arguments: One or more required arguments is null or empty" when performing user identity subject update via REST API
- OPENAM-19122: AM's jwks_uri endpoint should preserve order of keys within the set
- OPENAM-19123: AM validates duplicate registration tokens
- OPENAM-19171: Realm admin unable to call "policies?_action=evaluate"
- OPENAM-19190: LDAPAuthUtils for BASE_OBJECT does not work with special userId characters
- OPENAM-19208: Webhook with an empty url field throws NPE during a webhook session upgrade
- OPENAM-19220: WebAuthN/Fido - can not authenticate with recovery codes on Windows
- OPENAM-19281: OIDC dynamic client registration cannot handle "\n" in the client_description
- OPENAM-19290: In a cluster, changing AM debug level on local (AM2) to remote (AM1) does not have effect until restart of AM1
- OPENAM-19380: Social Google node does not work if placed after an input collector in a tree
- OPENAM-19455: Adding Authentication Context without Level value results in uneditable entity
- OPENAM-19506: Installer fails after pressing "cancel" button at amadmin password page
- OPENAM-19613: PSearch is already removed error message should be warning

### *Key Fixes in AM 6.5.4*

- OPENAM-11706: Policies in a policy set are not visible in Internet Explorer IE
- OPENAM-12503: SizeBasedRotationPolicy does not delete oldest file

- OPENAM-13586: Removing all SingleSignOnService entries from a hosted IDP entity causes it to vanish from the console (A Bad Federation entry makes other entries not listed)
- OPENAM-14240: FMSigProvider.verify does not tell if certificates are provided
- OPENAM-14245: Console error when adding entity to circle of trust
- OPENAM-14898: OTP Email Sender Authentication Node fails if no SMTP authentication credentials are specified
- OPENAM-15253: Upgrade fails if external data store for Applications and Policies is used
- OPENAM-15278: "Access Denied" error when accessing logout link and not currently signed in
- OPENAM-15501: Xml encryption 1.1 namespaces aren't always mapped to prefixes correctly
- OPENAM-15963: Historical retention files ( csv ) were not deleted
- OPENAM-16006: Device Code Grant does not work with Implied Consent as Authorization is not approved even after consented
- OPENAM-16216: Get Session Data node improvements
- OPENAM-16262: Javadocs for IdUtils needs updating
- OPENAM-16354: Concurrency bug in OAuth2ProviderSettingsFactory
- OPENAM-16368: Settings of Mail and Scripting global service properties are overwritten at upgrade
- OPENAM-16418: private_key_jwt client auth fails with 500 if claim format is wrong
- OPENAM-16472: Proxied Authentication fallback may not work when user entry lack some attributes
- OPENAM-16473: Unable to authenticate after UpdatePassword flow
- OPENAM-16535: "JWKs URI content cache miss cache time" is not triggered when "kid" is missing from cached JWK Set
- OPENAM-16540: Issues with Social Login URLs when navigating quickly between providers
- OPENAM-16556: Radius Server's does not log IP address into AM Audit logs
- OPENAM-16617: SuccessURL session property is set to gotoURL in authentication tree
- OPENAM-16642: Server id creation can fail when greater id is greater than 100
- OPENAM-16712: Importing SAML2 Metadata with both IDP and SP with cot ends up with duplicated extended metadata

- OPENAM-16745: client_id in access token ignores what's been registered when idm cache is disabled
- OPENAM-16838: AuthenticationApproachChecker does not handle session upgrade modules
- OPENAM-16847: AM email service failing with 'Start TLS' option
- OPENAM-16848: Choice Collector and WDSSO node combination does not work if whitelisting is enabled
- OPENAM-16849: WeChat Social Auth module broken (regression)
- OPENAM-16866: AM should fail gracefully if id_token fails to generate when swapping refresh token
- OPENAM-16876: Default ACR values on OIDC client profile is not honoured in order of preference
- OPENAM-16881: SAML federation library stopped supporting ACS URLs with query parameters
- OPENAM-16883: AM ignores AuthnRequestsSigned property during SSO
- OPENAM-16904: OIDC bearer module fails with NPE when id_token does not contain kid
- OPENAM-16910: Can not create SAML entity with entity id including a semicolon ';'
- OPENAM-16935: Logout issue after logging into AM with 'Remember my username' selected with iOS 14.0.1
- OPENAM-16936: Tree nodes create new keystore object each time node is called.
- OPENAM-16944: LdapDecisionNodes fails if inetuserstatus does not exist
- OPENAM-16955: When setCookieToAllDomains=false is used, a non matching request from other domain will fail
- OPENAM-16988: accessedEndpoint including port causes verify Assertion Consumer URL to fail
- OPENAM-16997: Device code grant implied consent fails if access_token request performed before user authenticates
- OPENAM-16998: Poor logging around failures "Invalid Assertion Consumer Location specified"
- OPENAM-17017: REST STS fails with unable get get sub-schema if cache is refreshed while updating REST config
- OPENAM-17034: In a realm if User Profile is set to Ignored the realm level Session Service quota settings is also ignored and only the Session Service setting at top level/global is evaluated
- OPENAM-17042: User Self Registration REST API does not generate SSO token
- OPENAM-17060: Audit Logging "Resolve host name" is still available after OPENAM-7849

- OPENAM-17070: SAML2 SP intiated SSO with AM as idp Proxy, RelayState is not returned from proxy after idp authentication
- OPENAM-17081: OAuth2 client agent group settings are not taken into account
- OPENAM-17089: Forgot password flow not working after initial attempt to reset password fails
- OPENAM-17097: Inconsistent scope policy evaluation between authorize and ROPC
- OPENAM-17114: Save Consent check box always shown, even when not configured
- OPENAM-17136: OAuth2 Dynamic Client Registration does not recognise recognised spec defined parameters
- OPENAM-17156: Adaptive Risk checkGeoLocation null countryCode can cause module fail.
- OPENAM-17157: Password reset via admin console with Proxied Authorization enabled is not possible
- OPENAM-17220: OAuthLogout.jsp compilation error isGotoUrlValid method signature not found
- OPENAM-17237: Using ODSEE on LDAP module for password reset, displays the wrong error message
- OPENAM-17242: OAuth2 Policy - Environment Condition AuthLevel >= doesn't work for ROPC grant
- OPENAM-17260: Allow arg=newsession usage in authorize calls
- OPENAM-17271: Typo for Realm in SAML/Federation debug
- OPENAM-17317: A realm without any modules can cause increased thread count and slow response.
- OPENAM-17320: Revisit prompt=login behaviour change that keeps existing session
- OPENAM-17322: SAML2 bearer grant returns NoUserExistsException
- OPENAM-17343: Access token call returns 500 error if password needs to be changed or has expired
- OPENAM-17349: OIDC Refresh token - Ops token is deleted from the CTS during refresh
- OPENAM-17357: Remote Consent Service RCS does follow RCS consented scope when authorization endpoint accessed without any scope
- OPENAM-17361: API Explorer Swagger Template body needs modification to include configExport, debugLogs and threadDump as per the API Documentation
- OPENAM-17364: prompt login / session upgrade / OIDC ACR looping with trees

- OPENAM-17365: Checking agent type with caller token can cause deadlock
- OPENAM-17395: SocialOpenIdConnectNode fails to recover from client's connection reset
- OPENAM-17396: Terms of Service URI Link does not Display in Consent Page
- OPENAM-17397: ssoadm can fail for some cloud-based setups due to FileBasedConfiguration check
- OPENAM-17405: Token introspection response not spec compliant
- OPENAM-17548: Can't go back to login page after invoking Social Authentication Nodes
- OPENAM-17587: OIDC bearer token authentication module requires context value setting for client secret
- OPENAM-17591: Session quota destroy next expiring action can fail when two new sessions attempt to read and update the same expiring session
- OPENAM-17610: OTP Email Sender node does not allow to specify connect timeout and IO/read timeout for underlying transport.
- OPENAM-17663: Improve the error response code for "Failed to revoke access token"
- OPENAM-17677: oauth2/device/code endpoint does not support locale parameter
- OPENAM-17678: Radius server fails to initialize on startup due to Config cache refreshed
- OPENAM-17683: Selfservice user registration auto login fails for a sub-realm
- OPENAM-17689: LDAPv3PersistentSearch should log when psearch connection is lost
- OPENAM-17691: lastEmailSent attribute missing when using am-identity-store setup profile
- OPENAM-17712: SAML2 session state not stored in-memory if it can't be stored locally
- OPENAM-17719: JATO Federation does not log trackingId in the audit log to permit traceability
- OPENAM-17782: Policy Eval fails with 400 error when user (subject) does not exist
- OPENAM-17783: Language tag limited to 5 characters instead of 8
- OPENAM-17784: Session timeouts (maximum session time, maximum idle timeout) set incorrectly if username is dynamically created in a tree.
- OPENAM-17793: OIDC pairwise subject not working when multiple redirect URIs configured with the same hostname
- OPENAM-17814: Auth Tree step-up fails if username case does not match
- OPENAM-17815: client specific token lifetimes are not used when casing of client id differs between authentication request and token request

- OPENAM-17826: introspect endpoint returns a static value for "expires_in" when using client based tokens
- OPENAM-17828: Apostrophe in username breaks Push/OATH device registration
- OPENAM-17896: ForgottenPassword Reset on multiple cluster not working when reset link clicked
- OPENAM-17916: When no session exists logout page redirects to login
- OPENAM-17954: Accept-Language header locale ignored on OAuth2 Consent page
- OPENAM-18009: AM return HTTP error code 500 when authenticate with authIndexType service without authIndexValue
- OPENAM-18017: Creation of UMA Policy to share a resource fails when identities have custom object classes
- OPENAM-18035: Policy retrieval of response attributes can fail when using LdapDecisionNode against different directory to identity store
- OPENAM-18043: Device Match module not setting correct AuthLevel
- OPENAM-18049: Saml2 Module does not handle the pipe delimeter
- OPENAM-18090: Creation of UMA Policy to share a resource fails when identities have custom attributes
- OPENAM-18091: Concurrent JATO COT updates can cause COT list inconsistencies
- OPENAM-18205: Excessive logging occurs when agent profile is not found
- OPENAM-18212: Check for user/agent profile condition during login can be refined further
- OPENAM-18235: IdPAdapter does not have access to IDPCache in preSendResponse hook when there is an existing session
- OPENAM-18316: Typo in oauth2 template (templates/touch/authorize.ftl)

### *Key Fixes in AM 6.5.3*

- OPENAM-9459: 500 Internal Server Error from changePassword endpoint with AD repo
- OPENAM-9777: Json Web Key URI in OAuth2 OpenID connect client config pre-populated incorrectly
- OPENAM-9931: Global Session Service - two fields with the exact same name (Redundant 'Global Attributes' setting should be removed)
- OPENAM-10843: When generating an OIDC token through STS a "kid" value is not specified

- OPENAM-10869: SAML2 Authentication module return "Unable to link local user to remote user" ambiguous.
- OPENAM-11159: OpenAM Amster export/import for Site have import errors
- OPENAM-11338: OpenID Connect id_token bearer auth module mixes up aud, azp during verification
- OPENAM-11912: LDAPv3 data store type does not handle property 'sun-idrepo-ldapv3-config-auth-kba-attr'
- OPENAM-11921: Incorrect NameId Format offered for SAML2 auth module in console
- OPENAM-12228: WebAgent REST API queryFilter expression does not work and acts all "true"
- OPENAM-12285: Allow Agents to receive notifications for oauth2 access token revocations
- OPENAM-12574: SAML2Utils.sendRequestToOrigServer throws NullPointerException on processing Cookies
- OPENAM-12759: During authorization code grant flow - max_age should be a number, not a string
- OPENAM-13310: Allow id tokens to be issued when no datastore configured
- OPENAM-13465: Dynamic client registration sets wrong subjectType
- OPENAM-13490: Software Publisher Agent - Secret is not saved when creating an Agent
- OPENAM-13549: Enabling Warning Headers causes multiple Secondary Configurations Tabs to generate 500 errors.
- OPENAM-13764: Monitoring logs in ERROR for "Agent.configAgentsOnly:agent type = OAuth2Client"
- OPENAM-13831: RP-Initiated Logout does not handle state parameter
- OPENAM-13840: Creating a Session service on a Subject fails when there is a realm Session service already
- OPENAM-13934: saml2error.jsp fails with exception when malformed SAML2 response given
- OPENAM-13948: When realm have Session service and user has Session service too viewing User's service fails
- OPENAM-14103: Session REST API does not offer same restricted session functionality as Session Client SDK API
- OPENAM-14109: Agent-as-OAuth2-Client cannot create id token when agent realm is different
- OPENAM-14188: Unable to Generate JSDoc in UI

- OPENAM-14229: custom AuthorizeTemplate under theme not used
- OPENAM-14265: Amster Import with --clean doesn't delete the secrets store and mappings
- OPENAM-14292: AM-LOGIN-COMPLETED does not log name of chain used for login
- OPENAM-14313: Audit Logging - STS transformations create duplicate entries
- OPENAM-14391: Self Service Link not displayed when using authentication tree
- OPENAM-14480: Provide better error handling during WDSSO Keytab file permission check
- OPENAM-14520: CreateMetadataModelImpl determines AM URL incorrectly when AM is deployed to root context
- OPENAM-14527: Microsoft Social Auth does not work with latest MS endpoints (Legacy OAuth2)
- OPENAM-14534: The request parameter should accept any signing algorithms supported by the OP
- OPENAM-14570: OAuth mTLS DN comparison fails when DER-encoding is different
- OPENAM-14682: Microsoft Social Auth fails when creating an Microsoft account (Legacy OAuth2)
- OPENAM-14700: XUI: AM pages don't render in Internet Explorer
- OPENAM-14744: Multivalued DN stops persistent search
- OPENAM-14782: AuthTree created Session does not use per User Session Service settings
- OPENAM-14841: WebAuthnAuthentication node inside a Page Node causes UI to fail rendering the tree
- OPENAM-14842: Misleading "CTS: Operation failed: Result Code: Connect Error" message when CTS store is still up and running
- OPENAM-14858: When NameIDPolicy does not contain `Format=..`, remoteEntityID is passed as null
- OPENAM-14867: AuthType is not set for Authentication Tree (AnyKnownUserAuthzModule fails in AuthTree)
- OPENAM-14874: It would be nice if the x-forwarded-* option was able to parse the comma-separated string and use the first (outermost) proxy host name.
- OPENAM-14883: OAuth2/OIDC - Issuing client secret to Public clients during registration
- OPENAM-14907: OAuth2/OIDC - jwk_uri returns keys for algorithms that are not listed/supported at the OAuth2 Provider
- OPENAM-14930: OAuth2 introspect fails with could not find any verification keys for keyId
- OPENAM-14951: OAuth2 provider does not validate RCS clients in an external application store

- OPENAM-14971: Unable to set up ssoadm when AM is installed to the root context
- OPENAM-14973: Monitoring throws StackTrace even if JDMK isn't being used/needed.
- OPENAM-14979: NPE in UtilProxySAMLAuthenticatorLookup if there is a failure to find cached oldSession in sessionUpgrade
- OPENAM-14995: IdP Initiated single logout only performs local logout if IdP session cannot be found in cache
- OPENAM-15012: OIDC - JWT Request Parameter returns errors in query, not in the fragment
- OPENAM-15018: Encrypted stateless tokens contains zip header, even though should not be present if none
- OPENAM-15028: Cannot load metadata in ssoadm without extended metadata
- OPENAM-15040: CIBA authorization request returns HTTP 500 NPE when file is wrong
- OPENAM-15044: OpenID connect id_token bearer Module Unable to obtain SSO Token due to OpenIDResolver Caching
- OPENAM-15049: wrong JWT while obtaining CIBA auth request id will result in HTTP 500 NPE
- OPENAM-15050: WebAuthn client script cannot be parsed in Internet Explorer
- OPENAM-15052: when id_token_hint is not JWT, CIBA authorization request returns HTTP 500
- OPENAM-15053: when client send wrong auth_req_id in CIBA polling request, there is HTTP 500 server error
- OPENAM-15063: when binding message of CIBA request is too long, notification fail to be sent
- OPENAM-15065: HTTP 500 authentication error in CIBA workflow when user deny request
- OPENAM-15073: Missing RelayState query parameter in the AM redirect to fedlet application
- OPENAM-15076: webAuthn config does not allow for multiple origins under the same rpId
- OPENAM-15089: SAML SLO - Allow RelayState to be a path-relative URL
- OPENAM-15105: Unable to get trusted devices using REST API
- OPENAM-15116: Auth ID jwt can be modified to determine whether a realm exists or not
- OPENAM-15117: KeyVault KeyStoreType not supported
- OPENAM-15121: Persistent Cookie Auth Tree does not work after the second relogin ( with browser closed )
- OPENAM-15128: webAuthn rpId detection does not account for cross-domain requests

- OPENAM-15129: registering client with token_endpoint_auth_method=none returns secret
- OPENAM-15145: OpenAM Scope Validator calls getUserInfo twice when creating IdToken
- OPENAM-15147: HTTP 500 upon accessing openam/json/
- OPENAM-15150: Upgrade fails when there is a bad Token Signing ECDSA public/private key pair alias field
- OPENAM-15160: LDAP Decision Node throws NPE when custom ldap server returns LDAP code 50 on bind
- OPENAM-15164: CDSSO with "ignore profile" throws "No OpenID Connect provider"
- OPENAM-15192: WebAuthn doesn't work on WildFly containers
- OPENAM-15193: moduleMessageEnabledInPasswordGrant is providing a different authentication error since AM 6.5.1
- OPENAM-15198: WS-FED Attribute Mapper returns incorrect map when AM is SP
- OPENAM-15206: webAuthn returns JavaScript with linebreak characters, and tries to store negative ints in an unsigned array
- OPENAM-15210: Authentication nodes that is assigned AuthType values may not work in Session Upgrade case with custom modules
- OPENAM-15216: LDAP Decision Node does not continue through "Fail" flow when Node Fails with exception
- OPENAM-15220: relayState is lost when both a relayState url and intermediate url are used
- OPENAM-15244: AM configuration does not perform schema extension for identity store although it has the permissions
- OPENAM-15257: XUI freezing when /authenticate returns unhandled http result codes
- OPENAM-15270: token_endpoint_auth_signing_alg should support any signing algorithms supported by the OP
- OPENAM-15303: Claims with multiple values in issued_token from REST STS represented inconsistently.
- OPENAM-15307: Trees Example is not working as expected OOTB to ?service=Example
- OPENAM-15309: JWTs are always SignedThenEncrypted when encrypted using JwtEncryptionHandler#encryptJwt
- OPENAM-15323: ROPC with tree throws "Internal Server Error (500)" when user credentials are incorrect using AuthTree

- OPENAM-15337: Change Advice Format Value
- OPENAM-15345: at_hash value generated does not take the latest modified access token
- OPENAM-15347: Trusted JWT Issuer is highlighted as current menu item when I choose OAuth2
- OPENAM-15349: Access Token request returns a 500 error
- OPENAM-15350: wrong message when saving Trusted JWT Issuer
- OPENAM-15353: OIDC Verification of a signed Jwt using multiple keys (e.g. jwk_uri) is not attempted against all keys
- OPENAM-15355: PageNode with multiple InputNodes without value throws Unsupported InputOnlyPasswordCallback
- OPENAM-15363: Redirect_uri_mismatch error occurs in Agent 5.x after upgrading from OpenAM 13.5.0
- OPENAM-15370: Ssoadm import-svc-cfg fails with Unable to obtain Server URL
- OPENAM-15371: Ssoadm import-svc-cfg fails with unable to recognize the data store type error
- OPENAM-15374: OpenID Client authentication with private_key_jwt and client_secret_jwt does not enforce required jti claims
- OPENAM-15382: custom Audit logging node or extending Scripted Node with able to audit
- OPENAM-15421: audit logging does not output when a collector node is wrapped in a page node
- OPENAM-15425: OIDC endsession - encrypted id_tokens are not supported
- OPENAM-15432: Oath User Devices endpoint not accessible for delegated admin
- OPENAM-15444: Prepare for Chrome's move to SameSite=lax by default
- OPENAM-15446: Incorrect error management during SAML SSO
- OPENAM-15459: When Encrypted Attributes on SP is set only with AutoFederation enabled, the attributes get decryption error
- OPENAM-15465: Sending HTTP Callback from Inner Tree Evaluator Fails Authentication
- OPENAM-15483: IDPSSOUtil.doSSOFederate throws NumberFormatException when subrealm is used with federation
- OPENAM-15487: OIDC - JWT Request Parameter returns errors in query, not in the fragment with invalid acr essential claim
- OPENAM-15489: WebAuthN Auth Node Doesn't Respect UV=Discouraged During AuthN

- OPENAM-15490: Policy evaluation and resource type lookups and creation fail and cannot recover from External Policy Store restart
- OPENAM-15491: Self service password reset returns 500 Internal Server Error, when new password rejected by datastore password policies.
- OPENAM-15494: AM expects nonce request parameter in authorize request when no id_token will be returned
- OPENAM-15507: 500 error when calling /revoke or /refresh endpoint with wrong token
- OPENAM-15508: moduleMessageEnabledInPasswordGrant does not apply to Trees
- OPENAM-15510: Generic amster error message "No Base Entity dc=config,dc=forgerock,dc=com found" needs to detail the actual ldap error - during install-openam
- OPENAM-15520: XUI Localisation Falls Back To AM-Default "EN" Instead Of Language-Default
- OPENAM-15530: OAuth2/OIDC - Resource Owner Password flow with a public client creates an AM session in CTS
- OPENAM-15533: WS-Federation doesn't work with Authentication Trees
- OPENAM-15548: WS-Fed - allow wreply to use Valid wreply List
- OPENAM-15559: OATH module broken in Japanese locale
- OPENAM-15562: SAML2 crosstalk fails when Accept-Language header is missing from the original request
- OPENAM-15574: Amster Import - updating com.iplanet.am.lbcookie.value to a different value to server ID
- OPENAM-15579: AM cookies are not set after successful SP-initiated SSO flow if SP Adapter calls 'response.sendRedirect(String)'
- OPENAM-15591: When using an OIDC id_token as SSO token composite/txid authenticate event generates 500
- OPENAM-15594: CsrfFilter should only block requests that contain a cookie
- OPENAM-15627: Switching CTS Storage Scheme to "Grant-set" fails with stateless refresh-tokens created with "One-To-One"
- OPENAM-15628: Grant-Set Storage Scheme for CTS does not work with CIBA Flow
- OPENAM-15632: OAuth2 Refresh token lifetime with -1 (never expires) cannot work with CTS TTL support
- OPENAM-15643: Need to send additional URL parameter values to agents from authorize end-point

- OPENAM-15645: The &refresh=true|false parameter for _action=validate is not working as expected
- OPENAM-15652: Debug.jsp does not update all existing appenders when trying to override -Dcom.iplanet.services.debug.level at runtime
- OPENAM-15662: RefreshToken does not work if Resource owner not in datastore (or using Ignore Profile)
- OPENAM-15663: UserInfoClaims is not part of public API
- OPENAM-15667: AM debug log does not tell which auth-module was handled - needed for troubleshooting
- OPENAM-15670: DeviceIdSave auth module initialization fails if username is null
- OPENAM-15671: LoginContext is missing debug logging for troubleshooting
- OPENAM-15679: The option "com.sun.am.ldap.connnection.idle.seconds" has a misspelling
- OPENAM-15687: Session endpoint is searching for a long value in CTS that is stored as a string
- OPENAM-15694: RestSTSServiceHttpRouteProvider causes memory leak by adding route for every access
- OPENAM-15696: The attribute "com.sun.am.ldap.connnection.idle.seconds" with > 0 causes LDAP pool initialization failure when using external CTS / UMA
- OPENAM-15697: Default ACR values from OAuth2 provider not taken into account
- OPENAM-15698: IdP-initiated SSO fails with error 'Error processing AuthnRequest. IDP Session is NULL'
- OPENAM-15713: AM SP drop the 80 characters RelayState silently for HTTP Redirect
- OPENAM-15722: SAML2 IdP federation endpoint does not set amlbcookie when using host-based cookies
- OPENAM-15724: SAML2 entities do not set amlbcookie if there is only one server
- OPENAM-15750: ERROR: OAuth2Monitor: Unable to increment "oauth2.grant" metric for unknown grant type BACK_CHANNEL
- OPENAM-15758: KeyStore Secret Store fails to start due to secretId having some special characters.
- OPENAM-15776: Push Registration fails (QR code invalid) to register
- OPENAM-15784: Form elements in policy environment condition tab are displayed twice
- OPENAM-15805: idtokeninfo endpoint gives invalid signature error when ID Token is expired

- OPENAM-15835: WebAuthn Nodes does not work when Relying Party domain is used.
- OPENAM-15841: DisableSameSiteCookiesFilter broken on WebLogic
- OPENAM-15849: An admin cannot DELETE 2fa devices owned by users
- OPENAM-15853: External UMA store fails on resource creation
- OPENAM-15855: AM requires "jti" claim for private_key_jwt client authentication
- OPENAM-15858: Auth Tree fails before 'Max Authentication Time' is reached if authentication session state management scheme CTS is used
- OPENAM-15864: SP init SSO fails after upgrade
- OPENAM-15881: Custom AM User (amUser.xml) field does not use default values from the schema
- OPENAM-15888: Long lived Device Code Lifetime cause Token's Expiry Time to be wrong
- OPENAM-15896: WS-Federation relying party initiated passive request - stuck at Account Realm selection
- OPENAM-15900: Kerberos fails when used with IBM JDK
- OPENAM-15905: Login failure with Post Authentication Plugin on timed out Authentication session throws NullPointerException
- OPENAM-15918: access_token endpoint returns wrong error if client is incorrect
- OPENAM-15919: AM OAuth metadata doesn't list revocation endpoint
- OPENAM-15929: OAuth2 Server Metadata - code challenge methods supported are not discoverable
- OPENAM-15944: WS-Federation - RPSignin Request fails because config data is used unchecked
- OPENAM-15970: Access Token introspect Fails in subrealm after root realm modified
- OPENAM-15977: _queryFilter is not working with _id field
- OPENAM-15979: WindowsDesktopSSO WSSO Configuration changes on isInitiator does not refresh configuration
- OPENAM-15982: OIDC - JWT Request Parameter returns errors in query, not in the fragment when consent is denied
- OPENAM-15989: OAuth2 client_id should be url-decoded when using basic auth
- OPENAM-16009: Windows Desktop SSO node full adoption and compliance with tree node specifications

- OPENAM-16013: Mismatched kid from Json Web Key URI when Specified Encryption Algorithm
- OPENAM-16014: An invalid user passed to any WebAuthn node throws NPE and breaks the Tree flow
- OPENAM-16031: Intermittent error message when concurrent obtain SSO Token ID with session quota constraints
- OPENAM-16032: Unable to delete devices with Recovery Code Collector Decision Node
- OPENAM-16036: Identity stores configuration broken after upgrade
- OPENAM-16049: WPA - Environment Condition TYPE!'s not working when evaluated to false
- OPENAM-16096: AMKeyProvider.mapPk2Cert error when using AWS CloudHSM
- OPENAM-16109: Non amadmin admin user can't edit Policy Sets / Policies
- OPENAM-16118: Deadlock in smIdmThreadPool notifyDescriptorChange
- OPENAM-16121: com.sun.identity.sm.notification.threadpool.size default should be updated to ensure sequential processing of SMS notifications
- OPENAM-16132: When TtlSupport is enabled, Stateless OAuth2 Refresh token and JWT whitelist fails on synchroniseExpiryDates
- OPENAM-16133: IdRepoCache being bypassed with increased usage of search alias
- OPENAM-16136: queryFilter only matches against first entry in array
- OPENAM-16137: JWT PAP claims problem with session upgrade
- OPENAM-16151: AM account lockout is checked even when it's disabled
- OPENAM-16152: After upgrade, new Identity page has duplicate 'new identity' field and email address does not save
- OPENAM-16157: Session Property Whitelist Service allows case variant Property Names but DS is not casesensitive
- OPENAM-16161: "same site patch" breaks SAML2 integrated mode on Apache Tomcat 7
- OPENAM-16164: social authmodule fails if OIDC provider uses algorithm RS256 to sign Id Token
- OPENAM-16165: social authmodule causes NullPointerException
- OPENAM-16177: Unmet lodash dependency warning when building openam-ui-ria module
- OPENAM-16184: Zero Page Login Collector does not work with UTF-8 base 64 encoded usernames and passwords

- OPENAM-16192: Elastic SAML: ForceAuthn fails if user already has a session when using Authentication tree
- OPENAM-16194: SAML jsp scripts do not compile
- OPENAM-16203: SAML SSO Admin Create SAML entities does not add attribute mappings
- OPENAM-16214: Push Authentication Module does not work on Session Upgrade when User Cache disabled
- OPENAM-16218: ERROR: OAuth2Monitor: Unable to increment "oauth2.grant" metric for unknown grant type JWT_BEARER
- OPENAM-16233: Policy evaluation fails when subject not found (even in ignore profile)
- OPENAM-16240: REST STS under subrealm cannot generate id_token with realm claim
- OPENAM-16242: Lowercase ID attribute does not work with OAuth2 settings.
- OPENAM-16249: AM expects consent_response although agent's configured for implied consent
- OPENAM-16251: OIDC authentication request with parameters 'prompt=none' and 'acr_values=' triggers authentication
- OPENAM-16256: StringIndexOutOfBoundsException when SAML Auth Request 's Reference URI has an empty string
- OPENAM-16268: Fedlet root url provider appends additional slash when context root is not available
- OPENAM-16271: Groovy Sandbox does need explicit whitelist on nested primitive Array type
- OPENAM-16279: AgentsRepo cannot recover when it fails especially on external Application store.
- OPENAM-16284: XUI does not handle Special Chars / UTF-8 in realms properly.
- OPENAM-16289: Fedlet fails with NPE when default digest method is missing from FederationConfig.properties
- OPENAM-16295: Watchdog errors on AM when external CTS with DS Entry Expiration and Deletion used
- OPENAM-16334: Checking AgentType with user token triggers permission check
- OPENAM-16338: Failing REQUISITE module after SUFFICIENT Device Match doesn't fail chain properly
- OPENAM-16342: Call to AdminTokenAction refreshes token in CTS datastore
- OPENAM-16343: ScriptCondition initializes AMIdentity with user token

- OPENAM-16345: Nullpointer exception AgentResourceExceptionMappingHandler when no errorCode
- OPENAM-16352: Policy evaluation performance degraded by 18-20%
- OPENAM-16367: OIDC request_uri response causes NPE while debug logging
- OPENAM-16379: URL fragments like # cause forbidden login in the XUI
- OPENAM-16394: Stress-testing increases am_cts_task_queue_count until a connection timeout
- OPENAM-16402: The passwordpolicy.allowDiagnosticMessage should be applicable to admin and selfservice password change.
- OPENAM-16418: private_key_jwt client auth fails with 500 if claim format is wrong
- OPENAM-16425: AM does not handle malformed/incorrect signature correctly
- OPENAM-16433: Audit Logging change of behaviour when capturing "principals" and "userid" data for each authentication entry.
- OPENAM-16450: 501 when default resource version set to "oldest" and Accept-API-Version header set
- OPENAM-16485: 'Failed Login URL' is not picked up from the auth chain
- OPENAM-16495: typo "Conenct" in Audience help of OpenID Connect id_token bearer authentication module
- OPENAM-16498: 500 returned when OAuth2 token is submitted with incorrect or non-existent KID
- OPENAM-16519: access_token call in OIDC flow cause search against Identity Store when Account Lockout is turned on and set to Store Invalid Attempts in Data Store
- OPENAM-16528: webauthn auth tempalte missing quotation marks aroudn userVerification component
- OPENAM-16537: AM not validating relative redirects on POST
- OPENAM-16551: Scalar String in OAuth2 Access Token Modification Script result in Unable to Obtain Access Token
- OPENAM-16555: (audit) logging does not tell which policy allowed or denied a resource request
- OPENAM-16566: OAuth2 Access token obtained from refresh token is certificate-bound regardless of "Certificate-Bound Access Tokens" configuration with POST authentication
- OPENAM-16583: Crucial information is missing when encountering LDAP connections issue.
- OPENAM-16684: OIDC Dynamic Registration client_description cannot take String type

- OPENAM-16697: Case mismatch for realm (when using legacy realm identifier format) on well-known endpoint results in issuer with incorrect path format
- OPENAM-16701: The authorize endpoint with a service parameter will cause the parameter to appear as a PAP claim in the agent's ID token

### *Key Fixes in AM 6.5.2.3*

- OPENAM-14951: OAuth2 provider does not validate RCS clients in an external application store
- OPENAM-15018: Encrypted stateless tokens contains zip header, even though should not be present if none
- OPENAM-15040: CIBA authorization request returns HTTP 500 NPE when file is wrong
- OPENAM-15052: when id_token_hint is not JWT, CIBA authorization request returns HTTP 500
- OPENAM-15053: when client send wrong auth_req_id in CIBA polling request, there is HTTP 500 server error
- OPENAM-15164: CDSSO with "ignore profile" throws "No OpenID Connect provider"
- OPENAM-15193: moduleMessageEnabledInPasswordGrant is providing a different authentication error since AM 6.5.1
- OPENAM-15444: Prepare for Chrome's move to SameSite=lax by default
- OPENAM-15446: Incorrect error management during SAML SSO
- OPENAM-15459: When Encrypted Attributes on SP is set only with AutoFederation enabled, the attributes get decryption error
- OPENAM-15465: Sending HTTP Callback from Inner Tree Evaluator Fails Authentication
- OPENAM-15490: Policy evaluation and resource type lookups and creation fail and cannot recover from External Policy Store restart
- OPENAM-15533: WS-Federation doesn't work with Authentication Trees
- OPENAM-15562: SAML2 crosstalk fails when Accept-Language header is missing from the original request
- OPENAM-15628: Grant-Set Storage Scheme for CTS does not work with CIBA Flow
- OPENAM-15697: Default ACR values from OAuth2 provider not taken into account
- OPENAM-15700: Dynamic user profile not working for chains
- OPENAM-15750: ERROR: OAuth2Monitor: Unable to increment "oauth2.grant" metric for unknown grant type BACK_CHANNEL

- OPENAM-15776: Push Registration fails (QR code invalid) to register on AM 6.5.2.2.
- OPENAM-15835: WebAuthn Nodes does not work when Relying Party domain is used.
- OPENAM-15841: DisableSameSiteCookiesFilter broken on WebLogic
- OPENAM-15858: Auth Tree fails before 'Max Authentication Time' is reached if authentication session state management scheme CTS is used

### *Key Fixes in AM 6.5.2.2*

- OPENAM-13934: saml2error.jsp fails with exception when malformed SAML2 response given
- OPENAM-14570: OAuth mTLS DN comparison fails when DER-encoding is different
- OPENAM-15050: WebAuthn client script cannot be parsed in Internet Explorer
- OPENAM-15145: OpenAM Scope Validator calls getUserInfo twice when creating IdToken
- OPENAM-15192: WebAuthn doesn't work on WildFly containers
- OPENAM-15323: ROPC with tree throws "Internal Server Error (500)" when user credentials are incorrect using AuthTree
- OPENAM-15345: at_hash value generated does not take the latest modified access token
- OPENAM-15355: PageNode with multiple InputNodes without value throws Unsupported InputOnlyPasswordCallback
- OPENAM-15363: Redirect_uri_mismatch error occurs in Agent 5.x after upgrading from OpenAM 13.5.0 to AM 6.5.2

### *Key Fixes in AM 6.5.2.1*

- OPENAM-9931: Global Session Service - two fields with the exact same name (Redundant 'Global Attributes' setting should be removed)
- OPENAM-14700: XUI: AM pages don't render in Internet Explorer
- OPENAM-14744: Multivalued DN stops persistent search
- OPENAM-14973: Monitoring throws StackTrace even if JDMK isn't being used/needed.
- OPENAM-15028: Cannot load metadata in ssoadm without extended metadata
- OPENAM-15063: Trusted JWT Issuer Agents fall under the 'Agents' group in XUI groupings - which doesn't match release notes
- OPENAM-15065: HTTP 500 authentication error in CIBA workflow when user deny request

- OPENAM-15105: Unable to get trusted devices using REST API
- OPENAM-15121: Persistent Cookie Auth Tree does not work after the second relogin ( with browser closed )
- OPENAM-15150: Upgrade fails when there is a bad Token Signing ECDSA public/private key pair alias field
- OPENAM-15347: Trusted JWT Issuer is highlighted as current menu item when I choose OAuth2
- OPENAM-15350: Wrong message when saving Trusted JWT Issuer

### *Key Fixes in AM 6.5.2*

- AM Can Now Parse JWTs With Non-String JOSE Header Parameters

  AM now parses JWTs containing non-string JWT header parameters, such as `jku` and `jwe`, but ignores the contents of the headers.
- OPENAM-10958: Amster cannot import configuration with containing sub realms with --clean if the instance already contains sub realms
- OPENAM-13402: Race condition in switch realm page display can sometimes result in displaying a login page
- OPENAM-13779: Session API - _action=refresh requires an admin token
- OPENAM-14022: We shouldn't be deploying Jetty inside a war file
- OPENAM-14054: XUI Custom templates and Partials not applied consistently
- OPENAM-14059: Inconsistent behavior while revoking stateful v/s stateless refresh tokens
- OPENAM-14138: Self registration url does not include realm parameter after upgrade from 13.5.1
- OPENAM-14213: Cannot view SAML SP entity imported from AWS in console
- OPENAM-14231: Passing in a JWT (with jku in the header) to the authorize endpoint fails
- OPENAM-14295: import-config fails when web-agent already present
- OPENAM-14310: CheckSession page indicates the session is not valid
- OPENAM-14337: Fail gracefully when request OIDC token using "Pairwise" Subject Type and no Redirection URI is configured in client
- OPENAM-14353: Error Message not Displayed when Change Password does not Meet Password Policy
- OPENAM-14356: Deleting OAuth 2.0 Client triggers unfiltered search

- OPENAM-14362: UMA load test fails with Invalid resource type error
- OPENAM-14419: Policy evaluation returns search results for all policies that match outside of specified application
- OPENAM-14464: XUI sends the following message "Loading custom partial "${partialPath}" failed. Falling back to default." to the browser console when a custom theme is used
- OPENAM-14466: Logs show MissingResource for key unableToCreateArtifactResponse during SAML2 login
- OPENAM-14483: If there is no token, then landing on the AM login page will result in 2 getSessionInfo Requests = 401 UnAuthZ
- OPENAM-14503: SAML2 - Key Transport Algorithm - RSA OAEP must be supported
- OPENAM-14523: NullPointerException in IdP-initiated ManageNameIDRequest using SOAP Binding
- OPENAM-14525: HSM secret store should not use the key alias as stable ID
- OPENAM-14539: SAML SLO with multi protocols
- OPENAM-14548: Consent page still shows what's been granted/removed as a result of OAuth2 scope policy evaluation
- OPENAM-14565: AM Upgrade NPE when unable to read operational attrs from directory
- OPENAM-14572: prompt=login destroys and creates new session
- OPENAM-14581: Handling ManageNameID fails if NameID does not include SPNameQualifier
- OPENAM-14642: OIDC Dynamic Client Registration registration_client_uri uses only Host header not BaseURL
- OPENAM-14643: OIDC Dynamic Client Registration registration_client_uri does not work for root realm
- OPENAM-14651: OAuth2 GrantSet E-Tag Assertion Failures due to Stale Reads
- OPENAM-14656: SAML redirect to login page on SP side fails if AM installed into the root context
- OPENAM-14685: PolicySetCacheImpl is not cleaned up correctly upon realm deletion
- OPENAM-14694: Consent page still shows claim values even when supported claim description is omit
- OPENAM-14707: ConsentRequiredResource class does not reuse value in Base url source service
- OPENAM-14715: Stateless token encryption does not work OOTB when upgrading from < AM 6.0

- OPENAM-14717: mailto attribute have space between ':' and mail address
- OPENAM-14740: idpSingleLogoutRedirect throws error 500 IllegalStateException on SLO
- OPENAM-14766: Introspect and tokeninfo endpoints return Internal Server Error 500 in some invalid tokens
- OPENAM-14783: PKCS11 KeyStore does not work on IBM JVM
- OPENAM-14784: AM cannot decrypt JWTs with CBC-HMAC encryption methods using a HSM
- OPENAM-14785: Give Authentication Nodes Access to the Request and Response
- OPENAM-14786: idpSingleLogoutPOST throws error 500 IllegalStateException on SLO
- OPENAM-14794: User privileges are removed from group if another group is given same privilege
- OPENAM-14798: Cannot always delete unused resource types in top level realm
- OPENAM-14799: Unable to update Agent profile using REST
- OPENAM-14821: Make HttpServletRequest/Response available from ExternalRequestContext
- OPENAM-14825: OAuth2 Dynamic Registration with Software Statement triggers objectClass=* search
- OPENAM-14829: AuthSchemeCondition doesn't return realm aware policy condition advice
- OPENAM-14840: Translation and help text missing for OAuth2 provider property `tokenEncryptionEnabled`
- OPENAM-14845: Userinfo endpoint does not correctly handle Certificate Bound Access Tokens
- OPENAM-14848: Insufficient debug logging in OpenID Connect authentication module
- OPENAM-14853: Intermittent bug caused by partials not being loaded in-time.
- OPENAM-14859: ROPC throws "Internal Server Error (500)" when 'Password Grant authentication service' is empty
- OPENAM-14865: No error message is provided when login page is supplied with incorrect session cookie domain
- OPENAM-14881: AM Proxied authorization feature on DataStore does not work with locked or expired DJ accounts for password change (gives errorcode=123)
- OPENAM-14889: Upgrade of Peristent Cookie auth module fails
- OPENAM-14901: XUI - SAML2 module doesn't redirect to IDP if it's 2nd in the chain
- OPENAM-14919: Unnecessary 'Unable to parse packet received from RADIUS client' log entries in log file

- OPENAM-14929: idpSSOInit error when session authLevel does not map to Auth Context
- OPENAM-14938: ID repo setAttributes service call returns the wrong error message with multiple datastores
- OPENAM-14940: Improve SAML2 Response/Assertion generation to not have carriage return inbetween XML tag
- OPENAM-14977: PKCE Code challenge method for Authorization Code if not set should use plain

### *Key Fixes in AM 6.5.1*

- OPENAM-5867: Data Store LDAP server (admin-ordered) list is reordered by OpenAM
- OPENAM-10127: SessionMonitoringStore should only be instantiated when monitoring is enabled
- OPENAM-11523: Using the LDAP/AD auth module, the change password on next login, if current password is empty it displays the wrong error message
- OPENAM-11863: CORSFilter position in web.xml should come before most filters
- OPENAM-12186: Introspect endpoint for RPT does not check the authorization scheme
- OPENAM-12498: Authorization Grant response returns scope(s) in the URL
- OPENAM-12620: Add more data to Scripted Node Decision binding
- OPENAM-12627: Initiating TransactionConditionAdvice with a wrong credential resulting in a non-error response
- OPENAM-12937: Soap STS creation fails when OpenIDConnect token config required
- OPENAM-12955: Resource Owner Password Credentials Grant does not work with trees
- OPENAM-12965: httpClient not exposed to OIDC Claim Script
- OPENAM-13000: Custom authentication module with a single ChoiceCallback value is processed without confirmation
- OPENAM-13088: Add option for isInitiator=false to WDSSO configuration
- OPENAM-13217: make transient state available to scripted node type
- OPENAM-13324: /users/{user}/devices/trusted REST queryFilter expression does not work and acts as "true"
- OPENAM-13446: Social Auth Service doesn't redirect if already using another chain
- OPENAM-13651: Client registration does not support auth method of "none"

- OPENAM-13720: Public API method LDAPUtils.convertToLDAPURLs can not handle IPv6 literals
- OPENAM-13851: Rest STS cannot be created in the Console when upgrading to 6
- OPENAM-13861: Social Authentication Tree does not complete its flow with ForceAuth parameter
- OPENAM-13892: Erroneous "Response's InResponseTo attribute is not valid error "SAML2 failover is enabled" when it is not
- OPENAM-13896: Comparison method violates its general contract! seen during amster import
- OPENAM-13900: OAuth2 Device flow - duplicate user_code error after authenticating user
- OPENAM-13940: Session quota limits not applied when using trees
- OPENAM-13941: OAuth2 Provider's ID Token Algs lists PS384 algorithm as PS284
- OPENAM-13978: Session Upgrade - AuthLevel format changes
- OPENAM-13991: 'issuer' value in .well-known/openid-configuration response is incorrect for a sub-realm
- OPENAM-14004: AM should support agents deployed to the root context (/), not just /openam
- OPENAM-14009: Authtree does not proceed for missing Authorization Header
- OPENAM-14032: In Social authentication nodes and Message node is not possible to change value of attribute maps or dictionaries
- OPENAM-14040: LdifUtils debug logging prints out wrong classname
- OPENAM-14049: Amster export failure
- OPENAM-14050: LDAP should reestablish connection to the orignal server after it has recovered
- OPENAM-14053: Cannot build openam-ui in Windows for Yarn using mvn
- OPENAM-14058: Cannot create Elasticsearch audit handler configuration through admin console UI
- OPENAM-14062: Redirect to Failure URL does not occur when authentication tree is not interactive
- OPENAM-14068: The new Policy and Application Stores only support a single target connection address
- OPENAM-14078: RetryTask can block notification processing for an extended period of time
- OPENAM-14080: LDAP Decision Node returns incorrect user attribute to search for in user store
- OPENAM-14082: Authentication Chains will not open using IE11

- OPENAM-14092: Custom node can prevent all default nodes appearing in admin view
- OPENAM-14111: Refresh Token flow not enabled on OAuth2 Client can still use Refresh Token flow
- OPENAM-14115: Sample Auth module does not work in a chain when used with Shared-state
- OPENAM-14147: arg=newsession in XUI does shows just the "Loading..." page
- OPENAM-14165: ThemeConfiguration is Not Exposed in Final UI Production Build
- OPENAM-14167: HTML tags are shown part of the messages in Change Password section of AD Authentication module.
- OPENAM-14169: XUI does not update for a new PollingWaitCallback
- OPENAM-14172: Amster Export - Persistent cookie Keystore Mapping inconsistency after upgrade to 6.5.0
- OPENAM-14174: AM shows Ldapter.delete exception when session expires is triggered
- OPENAM-14175: CTS updates on multivalue attributes may throws Duplicate values exception
- OPENAM-14183: Cannot change amadmin's password through XUI
- OPENAM-14189: effectiveRange of Time environment has issue
- OPENAM-14200: Social auth modules do not work when AM is installed into the root context
- OPENAM-14205: PageNodes property panel only appears for new PageNodes.
- OPENAM-14210: Unable to delete a PageNode that has child nodes
- OPENAM-14212: SAML redirect to login page fails if AM installed into the root context
- OPENAM-14222: Amster fails exporting Secret Store Mappings in sub-realms
- OPENAM-14232: Performance issue when creating resource_set in UMA with many existing resource_set
- OPENAM-14233: updated_at claim in the ID Token is returned as a string and not a number
- OPENAM-14235: mTLS drop down labels dont match the value (or the spec)
- OPENAM-14239: FMSigProvider.verify NPE with null input for certificates
- OPENAM-14255: Help text in OAuth 2.0 client "mTLS Self-Signed Certificate" property needs encoding?
- OPENAM-14270: SocialOpenIdConnectNodeTest does not compile
- OPENAM-14281: IdP Proxy relays wrong AuthnContextClassRef

- OPENAM-14307: ConcurrentModificationException when creating resource_set
- OPENAM-14308: LDAP Connection Pool Minimum Size for Identity Store missing from XUI
- OPENAM-14369: Upgrading from OpenAM 13.5.0 to AM 6.0.0.5 with custom PAPs causes NPE failure
- OPENAM-14374: Success login URL via trees redirects to profile when already authenticated
- OPENAM-14378: 'Set Persistent Cookie' node sets domain cookies in only one domain despite multiple Cookie Domains set
- OPENAM-14384: Allow metadata to be returned in authentication tree API responses
- OPENAM-14386: JWK keyuse can be customised
- OPENAM-14387: Dynamic registration PUT is not implemented
- OPENAM-14393: CTS Operation Fails Entry Already Exists logged for SAML2 Authentication is done
- OPENAM-14394: Customise the JWK KIDs
- OPENAM-14425: JwkSetSecretStore does not reload the SecretStore when it has expired
- OPENAM-14426: Unable to add external data store in AM (Policy | Application) when using TLS or SSL
- OPENAM-14427: Certificate Module with option "Match Certificate in LDAP" does not work in AM 6.5.0
- OPENAM-14450: userinfo typo in Claims.java
- OPENAM-14465: SAML2 Artifact binding fails on multi-instance / multiserver IDP setup with SAML2 Failover on
- OPENAM-14471: Failed to create root realm for data store (External Policy | Application)
- OPENAM-14505: Agent sessions are constrained by Session Quota
- OPENAM-14509: When a user is marked as inactive, can still perform introspect and tokeninfo endpoint requests
- OPENAM-14516: Attempt to resolve a named secret containing a `:` character on Windows fails if the filesystem secret store is involved
- OPENAM-14529: UMA RPT expiry time incorrect in CTS
- OPENAM-14546: SSOADM access not audited to the ssoadm.access logs anymore
- OPENAM-14573: amlbcookie is not secure when authenticating with trees

- OPENAM-14660: Error in console and unable to Add/Edit/Delete Security Questions for a user via XUI
- OPENAM-14669: ssoadm does not install using Java 1.8.192 and above
- OPENAM-14675: Error output in Configuration debug log when creating new realm

### *Key Fixes in AM 6.5.0.2*

- OPENAM-10127: SessionMonitoringStore should only be instantiated when monitoring is enabled
- OPENAM-11523: Using the LDAP/AD auth module, the change password on next login, if current password is empty it displays the wrong error messag
- OPENAM-13896: Comparison method violates its general contract! seen during amster import
- OPENAM-14009: Authtree does not proceed for missing Authorization Header
- OPENAM-14050: LDAP should reestablish connection to the orignal server after it has recovered
- OPENAM-14082: Authentication Chains will not open using IE11
- OPENAM-14111: Refresh Token flow not enabled on OAuth2 Client can still use Refresh Token flow
- OPENAM-14147: arg=newsession in XUI does shows just the "Loading..." page
- OPENAM-14189: effectiveRange of Time environment has issue
- OPENAM-14200: Social auth modules do not work when AM is installed into the root context
- OPENAM-14212: SAML redirect to login page fails if AM installed into the root context
- OPENAM-14222: Amster fails exporting Secret Store Mappings in sub-realms
- OPENAM-14281: IdP Proxy relays wrong AuthnContextClassRef
- OPENAM-14307: ConcurrentModificationException when creating resource_set
- OPENAM-14308: LDAP Connection Pool Minimum Size for Identity Store missing from XUI
- OPENAM-14336: Unable to use Signed Metadata to Re-Import
- OPENAM-14353: Error Message not Displayed when Change Password does not Meet Password Policy
- OPENAM-14378: 'Set Persistent Cookie' node sets domain cookies in only one domain despite multiple Cookie Domains set
- OPENAM-14386: JWK keyuse can be customised

- OPENAM-14393: CTS Operation Fails Entry Already Exists logged for SAML2 Authentication is done
- OPENAM-14425: JwkSetSecretStore does not reload the SecretStore when it has expired
- OPENAM-14427: Certificate Module with option "Match Certificate in LDAP" does not work in AM 6.5.0
- OPENAM-14505: Agent sessions are constrained by Session Quota
- OPENAM-14516: Attempt to resolve a named secret containing : character on Windows fail if the filesystem secret store is involved
- OPENAM-14572: prompt=login destroys and creates new session

### *Key Fixes in AM 6.5.0.1*

- OPENAM-12498: Authorization Grant response returns scope(s) in the URL
- OPENAM-12965: httpClient not exposed to OIDC Claim Script
- OPENAM-13446: Social Auth Service doesn't redirect if already using another chain
- OPENAM-13720: Public API method LDAPUtils.convertToLDAPURLs can not handle IPv6 literals
- OPENAM-13900: OAuth2 Device flow - duplicate user_code error after authenticating user
- OPENAM-13940: Session quota limits not applied when using trees
- OPENAM-13991: 'issuer' value in .well-known/openid-configuration response is incorrect for a sub-realm
- OPENAM-14049: Amster export failure
- OPENAM-14053: Cannot build openam-ui in Windows for Yarn using mvn
- OPENAM-14058: Cannot create Elasticsearch audit handler configuration through admin console UI
- OPENAM-14080: LDAP Decision Node returns incorrect user attribute to search for in user store
- OPENAM-14092: Custom node can prevent all default nodes appearing in admin view
- OPENAM-14165: ThemeConfiguration is Not Exposed in Final UI Production Build

### *Key Fixes in AM 6.5*

- OPENAM-13842: OAuth 2.0 Device flow - can no longer use `user_code` more than once.

- OPENAM-13786: REST policy evaluation throws 500 Internal Error due to stateless ssotoken encryption alg conflict.
- OPENAM-13774: SOAP STS for Delegation RelationShip Supported is always false on XUI.
- OPENAM-13732: Session Remaining Time is displayed with more precision and not rounded up.
- OPENAM-13712: Unknown Signing Algorithm when Client Based Session set Signing to NONE.
- OPENAM-13670: Selfservice password reset token doesn't work in site due to OPENAM-6426.
- OPENAM-13604: IdP Proxy relays wrong AuthnContextClassRef if the AuthLevel requested by the SP is not 0.
- OPENAM-13577: The `xmlsec 2.1.1.jar` had issues when linebreaks were enabled.
- OPENAM-13573: Concurrent changePassword requests to `LDAPAuthUtils` may cause "insufficient access rights" failures.
- OPENAM-13531: LDAP Decision node removed username from shared state when it is not found.
- OPENAM-13530: Datastore Decision node removed username from shared state when it is not found.
- OPENAM-13511: DN Cache should be cleared after idRepo config change.
- OPENAM-13496: Unable to view Services when some services have invalid attribute.
- OPENAM-13481: Stateless OAuth 2.0 Client_credential grant/implicit type has long CTS token timeout.
- OPENAM-13457: AM XUI favicon icon not being recognised.
- OPENAM-13456: AM XUI custom FooterTemplate.html and LoginHeaderTemplate.html was not being applied.
- OPENAM-13414: Upgrade fails if OAuth2 Provider service lacks `tokenSigningHmacSharedSecret`.
- OPENAM-13407: `AMIdentitySubject.isMember` should not check privilege for group in different realm.
- OPENAM-13359: P11RSAPrivateKey failed RSA key check.
- OPENAM-13318: Blank passwords using PageNode Auth Tree prevents log in.
- OPENAM-13316: LDAP Decision Node does not return Inactive Account result correctly in eDirectory.
- OPENAM-13308: LdapDecisionNode fails when Return UserDN to Datastore is set to false.
- OPENAM-13302: AM Self-registration kba threw an error when a user inputs an answer and pressed the enter key.

- OPENAM-13291: Create Identities Page appears broken after upgrade from 5.5 (to 6.0 or 6.5).
- OPENAM-13255: `DefaultIDPAccountMapper` does not append domain value for UPN.
- OPENAM-13249: AM did not recognize custom templates and partials.
- OPENAM-13183: Concurrent `changePassword` requests to the "users" REST endpoint caused "insufficient access rights" failures.
- OPENAM-13162: Policy evaluation returned 403 with expired stateless app token.
- OPENAM-13154: Lockout Duration Multiplier had no effect.
- OPENAM-13151: OAuth 2.0 Dynamic Registration did not accept Private-Use URI (for native apps) as `redirect_uri`.
- OPENAM-13128: Invalid error message was returned when user with expired password authenticated with persistent cookie module.
- OPENAM-13112: The `showServerConfig.jsp` page threw NullPointerException NPE when accessed using Site or LB URL.
- OPENAM-13100: LDAP Decision node fails with NPE when used with Active Directory.
- OPENAM-13087: ClassNotFound Exception thrown after upgrade.
- OPENAM-13085: WSFederation Active Request Profile authentication request hangs on input-less scripted modules.
- OPENAM-13082: Address claim in default OIDC claims script output non-spec compliant format.
- OPENAM-13080: Resource owners sharing resources to themselves caused an error message.
- OPENAM-13079: Importing SAML2 MetaData for RoleDescriptor for AttributeQueryDescriptor failed.
- OPENAM-13075: Incorrect message displayed when resource is being shared.
- OPENAM-13072: Case-sensitive usernames resulted in listing UMA resource incorrectly.
- OPENAM-13053: ScriptingService did not add the new values to whitelist during upgrade.
- OPENAM-12997: Consent for default scopes were not saved.
- OPENAM-12985: Debug log files were swamped with message 'LDAPUtils.isDN: Invalid DN' in 'error' level.
- OPENAM-12984: Access Token Endpoint issued search request against datastore for OAuth Client.
- OPENAM-12867: IdP-Proxy - Single Logout failed as LogoutResponse was not signed.

- OPENAM-12866: Subsequent idpSSOInit calls after the first will fail if custom IDPAdapter forces auth step up.
- OPENAM-12856: User authentication configuration not migrated to XUI.
- OPENAM-12847: Public API broken - SSOTokenManager.getValidSessions(SSOToken requester, String server).
- OPENAM-12801: OAuth 2.0 token signing forced PKCS#11 keys to have specific attributes.
- OPENAM-12784: ProviderConfiguration was not spec compliant.
- OPENAM-12770: Some SAML assertions were not deserialized from a SAML2 Token.
- OPENAM-12690: XUI theme configuration realm mapping was case sensitive.
- OPENAM-12625: JWT OIDC Token could not be valid for over 86400 seconds.
- OPENAM-12514: IdP initiated SSO - NumberFormatException was raised in session upgrade case.
- OPENAM-12506: Upgrade could fail with RemoveReferralsStep having too broad base DN.
- OPENAM-12419: Policy rules not updated when external configuration store connection restarted.
- OPENAM-12403: LDAP response controls are not logged which complicates troubleshooting.
- OPENAM-12401: DJLDAPv3Repo - insufficient debug logging to troubleshoot membership issues.
- OPENAM-12301: Account lockout logs ERROR: ISAccountLockout.getAcInfo: acInfo: null.
- OPENAM-12293: Audit logging no longer logs REST operation details.
- OPENAM-12209: The 'acr' and 'acr_sig' parameters can become duplicated during step-up authn, should not be present in url.
- OPENAM-12174: XUI - Deleting a built-in authentication module will delete any other created by it.
- OPENAM-12096: API explorer example for PUT on /global-config/services/scripting/contexts/{contexts}/engineConfiguration fails.
- OPENAM-11962: Calling Logout and passing a goto URL parameter with an expired session, goto URL is ignored.
- OPENAM-11665: Unable to login in XUI with users endpoint getting 404 due to KBA attribute issues.
- OPENAM-11642: CustomProperties do not work when creating J2EE/Web Agents via REST.
- OPENAM-11473: NumberFormatException on startup for External configuration setup.
- OPENAM-11407: An extra space in the CTS store connection string " openam.internal.example.com:50389" caused OpenDJ-SDK log to grow.

- OPENAM-11355: Missing Service tab when trying to configure dashboard with Active Directory datastore.
- OPENAM-11225: During single logout idpSingleLogoutRedirect threw 500 error.
- OPENAM-11177: Scripted auth module can not be used in auth chain if the username in shared state map does not 'match' the search attribute of the data store.
- OPENAM-11167: `<ActualLockoutDuration>` is not updated in the attribute sunStoreInvalidAttemptsData.
- OPENAM-11048: account lockout did not work when naming attribute and LDAP Users Search Attribute are different.
- OPENAM-10467: RFC7662: oauth2/introspect returned token_type not as Bearer.
- OPENAM-10296: Session UI only allows searching for users in datastore.
- OPENAM-9783: The json/users changePassword option returned the wrong error message with multiple datastores configured.
- OPENAM-8296: OAuth 2.0 consent screen does not use XUI theme configuration.
- OPENAM-4040: SSO failed between SPs in separate CoTs with same hosted IDP.

# Limitations

### *Limitations in AM 6.5*

The following limitations and workarounds apply to AM 6.5:

- Web Authentication (WebAuthn) Limitations

  AM 6.5 does not support the following functionality as described in the Web Authentication specification:

  #### *Registration*

  - Token Binding is not supported.
  - Web Authentication extensions are not supported.
  - Trust anchors are currently not supported.
  - Credential ID values are not verified against the credential IDs registered with all existing users.
  - The ECDAA signature of the Packed attestation format is not supported.

*Authentication*

- Token Binding is not supported.
- Web Authentication extensions are not supported.
- Signature counters are not supported.

For more information about Web Authentication, see "About Web Authentication (WebAuthn)" in the *Authentication and Single Sign-On Guide*.

- **RADIUS Service Only Supports Commons Audit Logging**. The new RADIUS service only supports the new Commons Audit Logging, available in this release. The RADIUS service cannot use the older Logging Service, available in releases prior to OpenAM 13.0.0.
- **Administration Console Access Requires the `Realm Admin` privilege**

  In this version of AM, administrators can use the AM console as follows:

  - Delegated administrators with the `Realm Admin` privilege can access full AM console functionality within the realms they can administer. In addition, delegated administrators in the Top Level Realm who have this privilege can access AM's global configuration.
  - Administrators with lesser privileges, such as the `Policy Admin` privilege, can not access the AM administration console.
  - The top-level administrator, such as `amadmin`, has access to full AM console functionality in all realms and can access AM's global configuration.

# Known Issues

The following important known issues remained open at the time release 6.5 became available. For details and information on other issues, see the issue tracker.

*Known Issues in AM 6.5.5*

- There are no new known issues in this release.

*Known Issues in AM 6.5.4*

- OPENAM-16976: Resource-based authentication does not evaluate policies in new policy set (not in default iPlanetAMWebAgentService)
- OPENAM-17198: "Illegal character in scheme name" error when creating client-based access and refresh tokens with client ID that contains special chars

- OPENAM-17203: With the OIDC Hybrid flow and implied consent on, scopes added by a customer scope validator are not available in claims script
- OPENAM-17245: 'User Attribute Mapping to Session Attribute' does not work for authentication trees
- OPENAM-17246: LDAP IdRepo - it's not possible to change the value of the 'LDAP Users Search Attribute' of an user identity subject via identity REST API
- OPENAM-17375: Social Auth Provider links only show on login page if using ldapService
- OPENAM-18034: Unable to set OAuth2Provider service attributes with ssoadm
- OPENAM-18039: WebAgent groups with 'Custom Properties' can not be managed via XUI-based AM console after upgrade
- OPENAM-18245: Creating a SAML2 entity with a double space results in SAML2 entity with a single space
- OPENAM-18268: webauthnDeviceProfiles is not multi value for AD
- OPENAM-18283: If IDP session is no longer valid, IDPSLO does not redirect to RelayState

### *Known Issues in AM 6.5.3*

- OPENAM-16223: Product nodes and marketplace/community/custom node cause naming clashes and prevent nodes with same name coinciding together
- OPENAM-15809: Update CORS service for IE11 compatibility
- OPENAM-15785: OIDC spec violation - HTTP POST can not be used to send Authentication Request
- OPENAM-14853: Intermittent bug caused by partials not being loaded in-time.
- OPENAM-14791: AM does not return scope attribute in response when granted scope is empty
- OPENAM-15431: Incorrect SHA-256 and DSA config in xml-security-config.xml
- OPENAM-15154: Update supported ID token encryption algorithms to include ECDH-ES
- OPENAM-16282: Upgrade may fails during upgrading SAML2 secret
- OPENAM-13942: SAML2 Circle of Trust - REST Update doesn't update the metadata of the provider
- OPENAM-16712: Importing SAML2 Metadata with both IDP and SP with cot ends up with duplicated extended metadata
- OPENAM-16703: OAuth2 Access token obtained from refresh token is certificate-bound regardless of "Certificate-Bound Access Tokens" configuration (when client_secret_basic used for credentials)
- OPENAM-15501: Xml encryption 1.1 namespaces aren't always mapped to prefixes correctly
- OPENAM-16540: Issues with Social Login URLs when navigating quickly between providers

- OPENAM-16745: client_id in access token ignores what's been registered when idm cache is disabled
- OPENAM-16669: IdentityGateway Agent entry missing attribute required to support org.forgerock.openam.agent.TokenRestrictionResolver#getAgentInfo
- OPENAM-15297: AM with Embedded DS - baseDN is hard-coded as dc

### *Known Issues in AM 6.5.2.3*

- Form Elements in Policy Environment Condition Tab Are Displayed Twice

  ForgeRock has found a small bug where form elements are displayed twice when specifying environment conditions for a policy. The workaround is to ignore the repeated form field. For more inforation, see OPENAM-15784: Form elements in policy environment condition tab are displayed twice.

- Kerberos Fails when Used with IBM JDK

  ForgeRock has found that the Windows-Desktop SSO (WSSO) module fails when used with IBM JDK. This is not known to be an issue with other JDKs. For more information, see OPENAM-15900: Kerberos fails when used with IBM JDK.

### *Known Issues in AM 6.5.2.2*

- There are no new known issues in this release.

### *Known Issues in AM 6.5.2.1*

- OPENAM-15370: ssoadm import-svc-cfg fails with Unable to obtain Server URL
- OPENAM-15371: ssoadm import-svc-cfg fails with unable to recognize the data store type error

### *Known Issues in AM 6.5.2*

- FRA-69: CIBA message is not displayed on Android 8.1.0
- OPENAM-15040: CIBA authorization request returns HTTP 500 NPE when file is wrong
- OPENAM-15049: wrong JWT while obtaining CIBA auth request id will result in HTTP 500 NPE
- OPENAM-15052: when id_token_hint is not JWT, CIBA authorization request returns HTTP 500
- OPENAM-15063: when there is quote in binding message of CIBA request, notification fail to be sent
- OPENAM-15064: HTTP 500 authentication error in CIBA workflow when user do not have registered mobile device

- OPENAM-15065: HTTP 500 authentication error in CIBA workflow when user deny request

### *Known Issues in AM 6.5.1*

- OPENAM-13905: XUI Authentication - Switching realms is not possible
- OPENAM-14666: XUI - InternalError: "too much recursion" error can appear when Adding/Viewing/Updating realms
- OPENAM-15006: A Choice collector inside a Page Node when re-opened does not show choices

### *Known Issues in AM 6.5.0.2*

- There are no known issues in this release, other than those identified in Known Issues in AM 6.5.

### *Known Issues in AM 6.5.0.1*

- There are no known issues in AM 6.5.0.1, other than those identified in Known Issues in AM 6.5.

### *Known Issues in AM 6.5*

- Non-String Header Parameters in JWTs Are Not Supported

  {am.abbr} does not support JWTs containing non-string header parameters, such as `jku` and `jwe` and therefore, it will not process such JWTs. AM will log a message similar to the following upon receiving a JWT with non-string header parameters:

  ```
  WARNING: An unexpected exception occurred while handling an OAuth2 request
  Internal Server Error (500) - The server encountered an unexpected condition which prevented it from
   fulfilling the request
  ```

  Do not send JWTs with non-string header parameters to AM; configure public keys/certificates in AM instead, as explained in the relevant sections of the documentation.

- **ssoadm** May Not Work with JDK 11 or JDK 1.8.0_192+

  In AM 6.5, **ssoadm** may not work with JDK 11 or JDK 1.8.0_192+ when AM is installed with DS in production mode or DS with restricted or strong ciphers.

  The workaround is to upgrade your AM deployment and tools to AM 6.5.0.

- Passwordless OAuth 2.0 Public Clients cannot choose `none` as Client Authentication Method

  As per RFC 7591, passwordless public client should be able to choose `none` as their client authentication method.

  At present, AM does not allow registering passwordless public clients with the `none` authentication method.

As a workaround, select the `client_secret_post` client authentication method when registering the client, but omit the password parameters when calling the endpoints. For example, do not use the `client_secret` parameter.

The `none` authentication method has been added to AM 6.5.1.

- **Using the Documented CORS Filter With IDM Integration Causes Errors**

  When configuring IDM to delegate authentication to AM, as described in the IDM *Samples Guide*, you must configure AM with a cross-origin resource sharing (CORS) filter.

  However, when you use a CORS filter based on the `org.forgerock.openam.cors.CORSFilter` filter class, Unexpected End of JSON Input errors occur.

  To work around the problem, configure AM's `web.xml` file as described in "Enabling CORS Support" in the *Installation Guide*, but use a CORS filter specific to the AM web container instead of using a filter based on the `org.forgerock.openam.cors.CORSFilter` filter class. For example, for Apache Tomcat, use a filter based on the `org.apache.catalina.filters.CorsFilter` filter class:

  - Add a `filter` clause similar to the following to the `web.xml` file, making sure to specify the correct URLs for your deployment in the `cors.allowed.origins` parameter:

```
<filter>
    <filter-name>CORSFilter</filter-name>
    <filter-class>org.apache.catalina.filters.CorsFilter</filter-class>
    <init-param>
        <param-name>cors.allowed.headers</param-name>
        <param-value>Content-Type,X-OpenIDM-OAuth-Login,X-OpenIDM-DataStoreToken,X-Requested-
With,Cache-Control,Accept-Language,accept,Origin,Access-Control-Request-Method,Access-Control-Request-
Headers,X-OpenAM-Username,X-OpenAM-Password,iPlanetDirectoryPro,Accept-API-Version</param-value>
    </init-param>
    <init-param>
        <param-name>cors.allowed.methods</param-name>
        <param-value>GET,POST,HEAD,OPTIONS,PUT,DELETE</param-value>
    </init-param>
    <init-param>
        <param-name>cors.allowed.origins</param-name>
        <param-value>https://openam.example.com:8443,https://openidm.example.com:8443</param-value>
    </init-param>
    <init-param>
        <param-name>cors.exposed.headers</param-name>
        <param-value>Access-Control-Allow-Origin,Access-Control-Allow-Credentials,Set-Cookie</param-
value>
    </init-param>
    <init-param>
        <param-name>cors.preflight.maxage</param-name>
        <param-value>10</param-value>
    </init-param>
    <init-param>
        <param-name>cors.support.credentials</param-name>
        <param-value>true</param-value>
    </init-param>
</filter>
```

- Add the following `filter-mapping` clause to the `web.xml` file:

```
<filter-mapping>
    <filter-name>CORSFilter</filter-name>
    <url-pattern>/json/*</url-pattern>
</filter-mapping>
```

- Large Amounts of Policies in a Policy Set Causes Errors if Unindexed

  If you have large numbers of policies in a policy set, ensure that the directory server has an index on the `sunxmlKeyValue` attribute.

  This index is created by default if you create an external DS instance by using the setup profiles feature. See "Preparing Policy and Application Stores" in the *Installation Guide*.

  If you did not use the setup profile feature to create the external DS instance, create an `equality` and `substring` index on the `sunxmlKeyValue` attribute. For example:

```
$ ./dsconfig \
 create-backend-index \
 --hostname external.example.com \
 --port 4444 \
 --bindDN "cn=Directory Manager" \
 --bindPassword "str0ngEx4mplePa55word" \
 --backend-name userRoot \
 --index-name sunxmlKeyValue \
 --set index-type:equality \
 --set index-type:substring \
 --trustAll \
 --no-prompt
```

  You will need to rebuild the indexes after adding additional attributes. For more information on creating indexes on attributes, and rebuilding indexes, see Indexing Attribute Values in the *Directory Services Administration Guide*.

- **Cached JavaScript Files from OpenAM 12.0.0 May Cause Redirect to undefined:8080**

  If you configure an OpenAM 12.0.0 instance with long-lived cache times for the `/XUI/index.html` file, you may experience unexpected redirects to `undefined:8080` after upgrading.

  To work around this issue, in your chosen web container, or proxy server, reconfigure the cache time for the `/XUI/index.html` file to be short-lived, for example, 5 minutes. Allow enough time that cached files with the long-lived cache time will have expired before upgrading.

  **Note**

  This issue does not affect upgrades from OpenAM 12.0.1 or later. OpenAM 12.0.1 and later set a short-lived `cache-control` header on UI files to work around the problem of having stale files cached locally.

- **OAuth2 Scopes Behavior Affected by Upgrade**

After an upgrade from OpenAM 12.0.x, OAuth v2.0 scope behavior uses a deprecated implementation class, `org.forgerock.openam.oauth2.provider.impl.ScopeImpl`.

The workaround is to manually update the OAuth v2.0 providers to use the `org.forgerock.openam.oauth2.OpenAMScopeValidator`.

For background information, see OPENAM-6319.

- **Supported ID Token Algorithms and Methods not Updated After Upgrade**

  AM 5 added additional algorithms and methods for encrypting ID tokens. Performing an upgrade from OpenAM 13.5 does not add these new values to the affected properties.

  After upgrade, navigate to *Realm Name* > Services > OAuth2 Provider > OpenID Connect, and manually update the ID Token Encryption Algorithms supported and ID Token Encryption Methods supported properties.

  For more information on the available algorithms and methods, see "Encrypting OpenID Connect ID Tokens" in the *OpenID Connect 1.0 Guide*.

- User Interface Not Localized if Locale Parameter Follows Fragment in URL

  The XUI user-facing pages are not localized if the `locale` parameter appears after the fragment in the URL.

  To ensure correct localization of user-facing pages, ensure the fragment appears at the end of the URL. For example:

  ```
  https://openam.example.com:8443/openam/XUI/?realm=/&locale=de#login
  ```

  For more information, see "Authenticating Using the XUI" in the *Authentication and Single Sign-On Guide*.

- OPENAM-3285: OpenID Connect authorization response is not returning required session_state.
- OPENAM-9098: Changes in `debugconfig.properties` do not take effect immediately.
- OPENAM-11706: Policies in a policy set are not visible in Internet Explorer IE
- OPENAM-12673: Title should display a translation text, not type in the radius sub configuration pages
- OPENAM-13428: EntitlementException not passed to PLL or JSON policy layer.
- OPENAM-13486: AM Upgrade fails on opendj_remove_session_listener_on_all_sessions.
- OPENAM-13583: OAuth 2.0 Node Redirect URL does not work.
- OPENAM-13836: Logout page is shown even when the server can't be contacted
- OPENAM-13885: When a user is deleted, two events are reported in the activity audit log

- OPENAM-13886: When a user is deleted, each user is removed from the group individually before the group is deleted
- OPENAM-13904: Authentication by using the REST API - Switching realms is not possible.
- OPENAM-13905: XUI Authentication - Switching realms is not possible.
- OPENAM-13912: All node implementations are loading the resource bundles incorrectly
- OPENAM-13937: AM stack trace in container logs
- OPENAM-13985: Authentication Devices Context (Settings) Menu if Off-Screen on Mobile
- OPENAM-14030: Enter will not submit New Tree form
- OPENAM-14047: SAML1 and ID-FF configuration should no longer be present
- OPENAM-14157: Move Remote Consent and Software Publisher agents under OAuth 2.0 heading
- OPENAM-14545: Debug log showing NullPointerException in com.sun.identity.federation.common.FSUtils#getRemoteServiceURLs
- OPENAM-15101: Remove the ability to disable XUI
- OPENAM-15659: WS-Federation IP incorrectly determines login URL when AM is deployed to root context
- OPENAM-16067: Potential memory leak when OAuth2 provider config changes
- OPENAM-16067: Potential memory leak when OAuth2 provider config changes

# Chapter 6
# Documentation Updates

The following table tracks changes to the documentation set following the release of AM 6.5:

*Documentation Change Log*

| Date | Description |
|---|---|
| 2022-08-02 | Initial release of AM 6.5.5.<br><br>In addition to the Release Note updates, the following changes were made to the documentation:<br><br>• Added guidance on protecting user profile attributes.<br><br>• Added documentation on the jwk_uri in the Remote Consent services configuration.<br><br>• Added a step to remove two Apache libraries after installation or upgrade.<br><br>• Added documentation on the `org.forgerock.openam.ldap.dncache.expire.time` advanced server property. |
| 2021-10-14 | Initial release of AM 6.5.4. |
| 2021-05-10 | The following changes were made to the documentation:<br><br>• Updated "Supported Clients" to mention that support for Internet Explorer 11 ends August 17, 2021, in alignment with the announcement from Microsoft ending support for Internet Explorer 11.<br><br>• Added additional information to the reference entry of the `/oauth2/authorize`'s request parameter.<br><br>• Updated Authentication Parameters to clarify that the `ForceAuth` parameter used with an authentication tree causes AM to issue a new session token, regardless of the security requirements.<br><br>• Updated Deprecated Functionality in AM 6.5 to clarify that the **ssoadm** command and the `configurator.jar`, `upgrade.jar`, and `ampassword` tools remain deprecated.<br><br>• Added a deprecation notice for Oracle WebLogic Server in Deprecated Functionality in AM 6.5.3, since it is unsupported in AM 7.<br><br>• Added an upgrade step to the To Upgrade From a Supported Version procedure to indicate that scripts must be upgraded manually. |

| Date | Description |
|---|---|
| 2020-12-07 | The following documentation updates were made:<br>• Added an entry in the Important Changes in AM 6.5.3 about changes to the SAML v2.0 `RelayState` redirection.<br>• Added an entry in the New Features in AM 6.5.3 about the new account active check authentication module.<br>• Added an entry in the New Features in AM 6.5.3 about the Audit Logging Service.<br>• Added an entry in the New Features in AM 6.5.3 about server-side scripts being able to redirect users to failure URLs.<br>• Added an entry in the Important Changes in AM 6.5.3 about changes pertaining to User Self-Service.<br>• Added an entry in the Important Changes in AM 6.5.3 about changes made to the JWK URI endpoint.<br>• Added the /oauth2/connect/jwk_uri section, which contains how to use the endpoint, how to customize key IDs, and how to deprecate and rotate keys.<br>• Added an entry in the Important Changes in AM 6.5.3 about changes to the `goto` and `gotoOnFail` parameter redirections.<br>• Added an entry in the Important Changes in AM 6.5.3 about changes to the `/json/authenticate` endpoint response when `HttpOnly` cookies are enabled.<br>• Added an entry in the Important Changes in AM 6.5.3 about changes to the SAML v2.0 Assertion Consumer Service.<br>• Corrected the user required to perform policy evaluation with REST in "Scripting a Policy Condition" in the *Authorization Guide*.<br>• Added documentation about HTTP options when configuring a JVM proxy in front of AM in "*Preparing for Deployment*" in the *Installation Guide*.<br>• Corrected the account mapper classes in "Configuring AM as an Authorization Server and Client" in the *OAuth 2.0 Guide*.<br>• Clarified the documentation about the OAuth 2.0 JWK URI cache settings in "Core" in the *OAuth 2.0 Guide*.<br>• Clarified the documentation about the SAML v2.0 hosted SP attribute map in "Hosted Service Provider Configuration Properties" in the *SAML v2.0 Guide*.<br>• Documented different commands to export policy and application store LDIF files in "Preparing Policy and Application Stores" in the *Installation Guide*.<br>• Added more information about how to configure the public key or HMAC secret in "Authenticating Clients Using JWT Profiles" in the *OAuth 2.0 Guide*. |

| Date | Description |
|---|---|
| | • Added information about how to determine if an existing session is present before using the "Get Session Data Node" in the *Authentication and Single Sign-On Guide*.<br>• Improved the documentation about tuning LDAP connections in nodes and modules in "Tuning LDAP Connectivity" in the *Setup and Maintenance Guide*.<br>• Added a known issue about JWTs containing non-string JOSE header parameters in Known Issues in AM 6.5. Also, added a partial fix for it in Key Fixes in AM 6.5.2.<br>• Added a table with the scripting versions that AM supports in "The Scripting Environment" in the *Development Guide*. |
| 2020-09-17 | The following documentation updates were made:<br>• Corrected the section "Linking Identities by Using an Authentication Chain" in the *SAML v2.0 Guide* to reflect it works for chains only, not authentication trees.<br>• Added an entry in the New Features in AM 6.5.3 about local storage support for SAML v2.0 Single Sign-on.<br>• Added an entry in the Important Changes in AM 6.5.3 about the `User Attribute Mapping to Session Attribute` and `Whitelisted Session Property Names` properties to retrieve user attributes in a session using REST. |
| 2020-09-16 | Initial release of AM 6.5.3.<br>The following documentation updates were made for this release:<br>• Add a link to the Deployment Planning Guide to recommend changing the `dsameuser` account at installation. See "Planning Security Hardening" in the *Deployment Planning Guide*.<br>• OAuth2 provider supported scopes property description changed from "Supported Scopes" to "Client Registration Scope Whitelist", which is the set of scopes allowed when registering clients dynamically with translations.<br>• Added a missing password change ACI in the external identity store. For more information, see "Installing and Configuring Directory Services for Identity Data" in the *Installation Guide*.<br>• Added CIBA binding_message limitations. For more information, see "*OAuth 2.0 Endpoints*" in the *OAuth 2.0 Guide*.<br>• Added a user store affinity load balancing option. For more information, see "Directory Services Configuration Properties" in the *Setup and Maintenance Guide*.<br>• Updated OIDC encryption documentation with ECDH-ES support. For more information, see "OAuth 2.0 and OpenID Connect 1.0 Client Settings" in the *OpenID Connect 1.0 Guide*. |

| Date | Description |
| --- | --- |
| | • Updated the Amster **:help *connect*** command section. For more information, see Connecting to Access Management.<br>• Added the **-t, --connection-timeout** in the Amster documentation. For more information, see First Steps.<br>• Added OPENAM-14503 to section 6.5.2 to the Release Notes.<br>• Added a "Restricting Endpoint Caching" section.<br>• Added anonymous session upgrade to the Authentication Tree "Anonymous User Mapping" node/component. For more information, see "Configuring Authentication Nodes" in the *Authentication and Single Sign-On Guide*.<br>• Fixed Base64 instead of Base64URL. For more information, see "*Implementing OAuth 2.0 Proof-of-Possession*" in the *OAuth 2.0 Guide*.<br>• Updated the Remote Consent Service section with the JWKS_URI location. For more information, see "OAuth 2.0 Remote Consent Service" in the *OAuth 2.0 Guide*.<br>• Updated the Basic Authentication section with URL-encoding characters. For more information, see "*Authenticating OAuth 2.0 Clients*" in the *OAuth 2.0 Guide*.<br>• Added Session Idle Timeout to client-based sessions limitations. For more information, see "*Implementing Sessions*" in the *Authentication and Single Sign-On Guide*.<br>• Added a section on the additional uses cased for ID tokens. For more information, see "*Additional Use Cases for ID Tokens*" in the *OpenID Connect 1.0 Guide*.<br>• Added a step to remove the `SLF4J` library before deploying on Wildfly 12+. For more information, see "Preparing for JBoss and WildFly" in the *Installation Guide*.<br>• Updated and reorganized the SAML v2.0 User Guide. For more information, see SAML v2.0 Guide.<br>• Updated amster install-openam errors. For more information, see Amster Users Guide.<br>• Updated the docs about keystore secrets store file location must be the same for all servers. For more information, see "*Configuring Secrets, Certificates, and Keys*" in the *Setup and Maintenance Guide*.<br>• Added a separate step to create base DN from bind user for UMA stores. For more information, see "Preparing External UMA Data Stores" in the *User-Managed Access (UMA) 2.0 Guide*.<br>• Updated the docs to mention custom scope validators. For more information, see "*About Upgrading*" in the *Upgrade Guide*. |

| Date | Description |
| --- | --- |
| | • Updated the docs to indicate that the access token modification script only works with a default scope validator. For more information, see "*Customizing OAuth 2.0*" in the *OAuth 2.0 Guide*.<br>• Updated the docs to indicate that the Data Store node does not lock accounts nor react to Behera password messages. For more information, see "Data Store Decision Node" in the *Authentication and Single Sign-On Guide*.<br>• Updated the Amster shell variables section. For more information, see Amster Users Guide.<br>• Added a step to change the cookie domain when configuring sites. For more information, see "Installing Multiple Servers" in the *Installation Guide*.<br>• Added a new `getSessionInfoAndResetIdleTime` endpoint. For more information, see "*Managing Sessions (REST)*" in the *Authentication and Single Sign-On Guide*.<br>• Added missing CTS Page and VLV Page Size properties. For more information, see "CTS Properties" in the *Reference*.<br>• Improved docs on keystore, bootstrap process, and removed bootstrap keystore. For more information, see "*Configuring Secrets, Certificates, and Keys*" in the *Setup and Maintenance Guide*.<br>• Added missing redirect URI from client setup. For more information, see "Authorization Code Grant with PKCE" in the *OpenID Connect 1.0 Guide*.<br>• Added SAML decryption logging properties. For more information, see "Using Fedlets in Java Web Applications" in the *SAML v2.0 Guide*.<br>• Added a note that JVM metric names may be unstable across releases. For more information, see "Monitoring Metrics" in the *Setup and Maintenance Guide*.<br>• Fixed an image in the SAML2 Guide. NameID Format in the *SAML v2.0 Guide*.<br>• Added a note that sample trees are only provided when AM is installed with the embedded config store. For more information, see "Configuring Authentication Trees" in the *Authentication and Single Sign-On Guide*.<br>• Added info about boot.json and the bootstrap process. For more information, see "Installing Multiple Servers" in the *Installation Guide*.<br>• Clarified the config change notification behavior. For more information, see "SDK Properties" in the *Reference*.<br>• Changed the default for SMS notifications to make it sequential. For more information, see "Tuning an Instance" in the *Setup and Maintenance Guide*.<br>• Corrected UMA requesting party access diagram and text. For more information, see "*Introducing UMA 2.0*" in the *User-Managed Access (UMA) 2.0 Guide*. |

| Date | Description |
|---|---|
| | • Corrected CTS reaping property names. For more information, see "*Implementing the Core Token Service*" in the *Installation Guide*.<br>• Added Groovy/Javascript capabilities and limitations in scripted decision node. For more information, see "The Scripting Environment" in the *Development Guide*.<br>• Updated docs to show how to configure amr mappings with authentication trees. For more information, see "*Adding Authentication Requirements to ID Tokens*" in the *OpenID Connect 1.0 Guide*.<br>• Added text that the Json Web Key URI field is now empty when creating an Oauth2 client. For more information, see "OAuth 2.0 and OpenID Connect 1.0 Client Settings" in the *OAuth 2.0 Guide*.<br>• Changed references to http.headers to http.request.headers. For more information, see "Audit Logging File Format" in the *Setup and Maintenance Guide*.<br>• Changed the authentication code grant documentation to show the right requirements and the right type of tokens it returns For more information, see "Authorization Code Grant" in the *OAuth 2.0 Guide*. |
| 2020-05-27 | Updated and improved the documentation around keystores, secret stores, and the AM startup process.<br><br>As part of this change, the advice about creating a bootstrap keystore separated from the AM keystore given as part of 6.5.x has been removed. It has been replaced with new, easier to use and maintain instructions to create a new AM keystore that doubles up as the bootstrap keystore. |
| 2020-03-25 | Added a release note for 6.5.1. This version added support for the `none` authentication method for OpenID Connect clients.<br><br>For more information, see Important Changes in AM 6.5.1. |
| 2020-02-17 | Initial release of AM 6.5.2.3. |
| 2020-01-06 | Updated SAML v2.0 Guide<br><br>The SAML v2.0 Guide has been reorganized and improved. |
| 2019-10-31 | Initial release of AM 6.5.2.2.<br><br>The following documentation updates were made for this release:<br>• Updated Base64URL-encoded DER certificate string. For more information, see "JWK-Based Proof-of-Possession" in the *OAuth 2.0 Guide*.<br>• Updated the documentation to clarify how secret stores resolve secrets. For more information, see "*Configuring Secrets, Certificates, and Keys*" in the *Setup and Maintenance Guide*. |
| 2019-08-27 | Initial release of AM 6.5.2.1. |
| 2019-06-14 | Initial release of AM 6.5.2. |

| Date | Description |
|---|---|
| | The following documentation updates were made for this release:<br>• Added a note about exporting Amster configuration files after running an upgrade to AM 6.5.0, or from AM 6.5.0/6.5.0.x to AM 6.5.x (for example, AM 6.5.1 or 6.5.2). For more information, see "Upgrade Paths" in this Release Notes or "*Upgrading AM Instances*" in the *Upgrade Guide*.<br>• Updated the procedure for configuring external policy and applications stores. You can now specify multiple URLs, with either active-passive or affinity connectivity. For more information, see "To Connect AM to an External Policy or Application Store" in the *Setup and Maintenance Guide*.<br>• Added an important change in 6.5.1 release notes about the OAuth 2.0/OpenID Connect provider requiring clients to pre-register their `request_uri` values. |
| 2019-05-07 | The restriction against implementing SAML v2.0 single sign-on (SSO) and single logout (SLO) when running AM with client-based sessions has been updated. For more information, see "Session State Considerations" in the *SAML v2.0 Guide*. |
| 2019-04-26 | Initial release of AM 6.5.0.2. |
| 2019-04-11 | Initial release of AM 6.5.1.<br>The following documentation updates were made for this release:<br>• Added a note to the What's New section for AM 6.5.0 about a new OAuth 2.0 access token claim, `"cts"`. See What's New in AM 6.5.<br>• Added documentation on OAuth 2.0 Mutual TLS support. See "Authenticating Clients Using Mutual TLS" in the *OAuth 2.0 Guide*.<br>• Added documentation on the OAuth 2.0 Dynamic Client Registration Management Protocol. "Dynamic Client Registration Management" in the *OAuth 2.0 Guide*.<br>• Added a footnote on WebAuth tree. See "WebAuthn Registration Node" in the *Authentication and Single Sign-On Guide*.<br>• Fixed a link in the procedure in the section, *To Install and Configure Directory Services for Identity Data*. See "To Install and Configure Directory Services for Identity Data" in the *Installation Guide*.<br>• Added a footnote on the limitations of Java 11. See "Java Requirements".<br>• Removed the note recommending using AM embedded DS server as the configration data store. We recommend implementing an external configuration store. See "Back End Directory Servers" in the *Deployment Planning Guide*.<br>• Updated the images in the Deployment Planning Guide. See "*Example Deployment Topology*" in the *Deployment Planning Guide*.<br>• Updated documentation on upgrading and configuring secret stores. See "Installing Multiple Servers" in the *Installation Guide*, Secret Store Changes |

| Date | Description |
|---|---|
| | After Upgrade in the *Setup and Maintenance Guide*, "To Redeploy Secret Stores to a Site After Upgrade" in the *Upgrade Guide*.<br>• Updated UMA urls in the *User Managed Access Guide*. See "*Using UMA 2.0*" in the *User-Managed Access (UMA) 2.0 Guide*.<br>• Added a tip about account lockout only counting `InvalidPasswordException`. See "The Sample Authentication Logic" in the *Authentication and Single Sign-On Guide*.<br>• Removed list of endpoint versions in favor of API Explorer. See "REST API Versioning" in the *Authentication and Single Sign-On Guide*.<br>• Documented that LDAP user and group container property can be empty. See "Generic LDAPv3 Configuration Properties" in the *Setup and Maintenance Guide*.<br>• Improved the keystore section. See "*Configuring Secrets, Certificates, and Keys*" in the *Setup and Maintenance Guide*.<br>• Duplicated script API sections to the Dev Guide. See "*Developing with Scripts*" in the *Development Guide*.<br>• Updated the folder references in the UI Customization Guide. See "*Reference*" in the *UI Customization Guide*.<br>• Documented the key ID customization extension endpoint. See "Customizing Public Key IDs" in the *OpenID Connect 1.0 Guide*.<br>• Updated section on blacklisting client-based tokens to mention the whitelist used by refresh tokens, and added to release notes. See "Configuring Client-Based OAuth 2.0 Token Blacklisting" in the *OAuth 2.0 Guide*. |
| 2019-02-19 | Added missing release note for 6.5.0 regarding a change to the paths of the source code of the UI. For more information, see Important Changes in AM 6.5. |
| 2019-01-28 | Added support for audit logging to a PostgreSQL database. For more information, see "Implementing JDBC Audit Event Handlers" in the *Setup and Maintenance Guide*. |
| 2019-01-22 | Added how to validate CSV logs configured for the detection of tampering. For more information, see "Configuring CSV Audit Event Handlers" in the *Setup and Maintenance Guide*. |
| 2019-01-17 | Initial release of AM 6.5.0.1. |
| 2018-11-30 | Initial release of AM 6.5.<br>Added new Authentication Node Development Guide.<br>The following documentation updates were made in this release:<br>• Duplicated scripting API documentation to the Development Guide. |

| Date | Description |
| --- | --- |
| | • The Windows NT authentication module was deprecated in this release and no longer appears in the "Configuring Authentication Modules" in the *Authentication and Single Sign-On Guide*. |

# Appendix A. Release Levels and Interface Stability

This appendix includes ForgeRock definitions for product release levels and interface stability.

## ForgeRock Product Release Levels

ForgeRock defines Major, Minor, Maintenance, and Patch product release levels. The release level is reflected in the version number. The release level tells you what sort of compatibility changes to expect.

*Release Level Definitions*

| Release Label | Version Numbers | Characteristics |
|---|---|---|
| Major | Version: x[.0.0] (trailing 0s are optional) | • Bring major new features, minor features, and bug fixes<br>• Can include changes even to Stable interfaces<br>• Can remove previously Deprecated functionality, and in rare cases remove Evolving functionality that has not been explicitly Deprecated<br>• Include changes present in previous Minor and Maintenance releases |
| Minor | Version: x.y[.0] (trailing 0s are optional) | • Bring minor features, and bug fixes |

| Release Label | Version Numbers | Characteristics |
|---|---|---|
| | | • Can include backwards-compatible changes to Stable interfaces in the same Major release, and incompatible changes to Evolving interfaces<br>• Can remove previously Deprecated functionality<br>• Include changes present in previous Minor and Maintenance releases |
| Maintenance, Patch | Version: x.y.z[.p]<br>The optional `.p` reflects a Patch version. | • Bring bug fixes<br>• Are intended to be fully compatible with previous versions from the same Minor release |

# ForgeRock Product Stability Labels

ForgeRock products support many features, protocols, APIs, GUIs, and command-line interfaces. Some of these are standard and very stable. Others offer new functionality that is continuing to evolve.

ForgeRock acknowledges that you invest in these features and interfaces, and therefore must know when and how ForgeRock expects them to change. For that reason, ForgeRock defines stability labels and uses these definitions in ForgeRock products.

*ForgeRock Stability Label Definitions*

| Stability Label | Definition |
|---|---|
| Stable | This documented feature or interface is expected to undergo backwards-compatible changes only for major releases. Changes may be announced at least one minor release before they take effect. |
| Evolving | This documented feature or interface is continuing to evolve and so is expected to change, potentially in backwards-incompatible ways even in a minor release. Changes are documented at the time of product release.<br>While new protocols and APIs are still in the process of standardization, they are Evolving. This applies for example to recent Internet-Draft implementations, and also to newly developed functionality. |
| Legacy | This feature or interface has been replaced with an improved version, and is no longer receiving development effort from ForgeRock.<br>You should migrate to the newer version, however the existing functionality will remain.<br>Legacy features or interfaces will be marked as *Deprecated* if they are scheduled to be removed from the product. |

| Stability Label | Definition |
|---|---|
| Deprecated | This feature or interface is deprecated and likely to be removed in a future release. For previously stable features or interfaces, the change was likely announced in a previous release. Deprecated features or interfaces will be removed from ForgeRock products. |
| Removed | This feature or interface was deprecated in a previous release and has now been removed from the product. |
| Technology Preview | Technology previews provide access to new features that are considered as new technology that is not yet supported. Technology preview features may be functionally incomplete and the function as implemented is subject to change without notice. DO NOT DEPLOY A TECHNOLOGY PREVIEW INTO A PRODUCTION ENVIRONMENT.<br><br>Customers are encouraged to test drive the technology preview features in a non-production environment and are welcome to make comments and suggestions about the features in the associated forums.<br><br>ForgeRock does not guarantee that a technology preview feature will be present in future releases, the final complete version of the feature is liable to change between preview and the final version. Once a technology preview moves into the completed version, said feature will become part of the ForgeRock platform. Technology previews are provided on an “AS-IS” basis for evaluation purposes only and ForgeRock accepts no liability or obligations for the use thereof. |
| Internal/Undocumented | Internal and undocumented features or interfaces can change without notice. If you depend on one of these features or interfaces, contact ForgeRock support or email info@forgerock.com to discuss your needs. |

# Appendix B. Getting Support

ForgeRock provides support services, professional services, training through ForgeRock University, and partner services to assist you in setting up and maintaining your deployments. For a general overview of these services, see https://www.forgerock.com.

ForgeRock has staff members around the globe who support our international customers and partners. For details on ForgeRock's support offering, including support plans and service level agreements (SLAs), visit https://www.forgerock.com/support.

ForgeRock publishes comprehensive documentation online:

- The ForgeRock Knowledge Base offers a large and increasing number of up-to-date, practical articles that help you deploy and manage ForgeRock software.

  While many articles are visible to community members, ForgeRock customers have access to much more, including advanced information for customers using ForgeRock software in a mission-critical capacity.

- ForgeRock product documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It is visible to everyone and covers all product features and examples of how to use them.